Benutzerhandbuch - Deutsch

FUJITSU Software ServerView Suite

Benutzerverwaltung in ServerView 6.30

Zentrale Authentifizierung und rollenbasierte Autorisierung

Ausgabe März 2014

Kritik… Anregungen… Korrekturen…

Die Redaktion ist interessiert an Ihren Kommentaren zu diesem Handbuch. Ihre Rückmeldungen helfen uns, die Dokumentation zu optimieren und auf Ihre Wünsche und Bedürfnisse abzustimmen.

Sie können uns Ihre Kommentare per E-Mail an manuals@ts.fujitsu.com senden.

Zertifizierte Dokumentation nach DIN EN ISO 9001:2000

Um eine gleichbleibend hohe Qualität und Anwenderfreundlichkeit zu gewährleisten, wurde diese Dokumentation nach den Vorgaben eines Qualitätsmanagementsystems erstellt, welches die Forderungen der DIN EN ISO 9001:2000 erfüllt.

cognitas. Gesellschaft für Technik-Dokumentation mbH
www.cognitas.de

Copyright und Handelsmarken

Copyright © 2014 Fujitsu Technology Solutions GmbH.

Alle Rechte vorbehalten.
Liefermöglichkeiten und technische Änderungen vorbehalten.

Alle verwendeten Hard- und Softwarenamen sind Handelsnamen und/oder Warenzeichen der jeweiligen Hersteller.

Inhalt

1 Einleitung 11

1.1 Autorisierungs- und Authentifizierungskonzept 11
1.2 Zielgruppen und Zielsetzung des Handbuchs 12
1.3 Struktur des Handbuchs 13
1.4 Änderungen seit der vorherigen Ausgabe des Handbuchs . 14
1.5 ServerView Suite Link-Sammlung 15
1.6 Dokumentation zur ServerView Suite 16
1.7 Darstellungsmittel 18

2 Benutzerverwaltung und Sicherheitsarchitektur (Überblick) 19

2.1 Voraussetzungen 20
2.2 Globale Benutzerverwaltung mit LDAP-Verzeichnisdienst . 22
2.2.1 Vorteile durch Verwendung eines Verzeichnisdienstes 22
2.2.2 Unterstützte Verzeichnisdienste 23
2.2.3 Open DS oder einen bereits vorhandenen, konfigurierten Verzeichnisdienst verwenden 24
2.2.4 Gemeinsame Benutzerverwaltung für ServerView Suite und iRMC S2/S3/S4 25
2.3 Rollenbasierte Zugangskontrolle (RBAC) 26
2.3.1 Benutzer, Benutzerrollen und Berechtigungen (Privilegien) . . . 26
2.3.2 RBAC-Implementierung in OpenDJ 27
2.3.3 RBAC bei einem bereits existierenden konfigurierten Verzeichnisdienst 28
2.4 Single Sign-on (SSO) mithilfe eines CAS Service 29
2.4.1 CAS-basierte SSO-Architektur 30
2.4.2 Single Sign-on aus Sicht des Benutzers 33

3 ServerView-Benutzerverwaltung mit LDAP-Verzeichnisdienst 35

3.1 Zugang zum Verzeichnisdienst konfigurieren 35

3.2 ServerView-Benutzerverwaltung mit OpenDJ 36
3.2.1 Vordefinierte Benutzer und Rollen 36
3.2.2 Passwörter der vordefinierten Benutzer definieren/ändern 38
3.2.2.1 Passwort des OpenDJ Directory Managers 38
3.2.2.2 Passwort von svuser definieren / ändern. 41
3.2.2.3 Vordefinierte Passwörter der vordefinierten Benutzer Administrator, Monitor, Operator und UserManager ändern. . 43
3.2.3 LDAP-Portnummern von OpenDJ ändern 44
3.2.3.1 LDAP-Portnummern auf Windows Systemen ändern 44
3.2.3.2 LDAP-Portnummern auf Linux Systemen ändern 45
3.2.4 Benutzer, Rollen und Berechtigungen in OpenDJ verwalten . . . 46
3.2.4.1 ServerView User Management starten. 47
3.2.4.2 Eigenes OpenDJ-Passwort ändern 48
3.2.4.3 User Management-Wizard 49
3.2.5 iRMC S2/S3/S4 in die ServerView-Benutzerverwaltung mit OpenDJ und SSO integrieren 58
3.2.5.1 iRMC S2/S3/S4 in die ServerView-Benutzerverwaltung mit OpenDJ und SSO integrieren 58
3.2.5.2 iRMC S2/S3/S4-Web-Oberfläche für CAS-basierte Single Sign-on (SSO)-Authentifizierung konfigurieren. 61
3.2.6 OpenDJ-Daten sichern und wiederherstellen 63
3.2.6.1 OpenDJ-Daten auf Windows-Systemen sichern und wiederherstellen 63
3.2.6.2 OpenDJ-Daten auf Linux-Systemen sichern und wiederherstellen 64

3.3 ServerView-Benutzerverwaltung in Microsoft Active Directory integrieren 65
3.3.1 Passwort des LDAP-Bind-Kontos ändern 75
3.3.2 LDAP Password Policy Enforcement (LPPE) 76

4 SSL-Zertifikate für Authentifizierung verwalten 81

4.1 SSL-Zertifikate verwalten (Überblick) 82

4.2 SSL-Zertifikate auf der Management-Station verwalten . . . 85
4.2.1 Bei der Installation wird automatisch ein selbstsigniertes Zertifikat erzeugt 85

4.2.2 Zertifizierungsstellenzertifikat (CA Certificate) erzeugen 87
4.2.3 Software-Tools zur Zertifikats- und Schlüsselverwaltung 89
4.2.4 Zertifikat auf der zentralen Management-Station ersetzen . . . 90
4.2.4.1 Zertifikat auf einem Windows System ersetzen 91
4.2.4.2 Zertifikat auf einem Linux System ersetzen 96

4.3 Verwalteten Server Systeme für Role Based Access (RBAC) und Client-Authentifizierung einrichten 101
4.3.1 Dateien <system_name>.scs.pem und <system_name>.scs.xml auf den verwalteten Server übertragen 101
4.3.2 Zertifikatsdateien auf einem Windows System installieren . . . 103
4.3.2.1 Zertifikatsdateien gemeinsam mit den ServerView Agenten installieren 103
4.3.2.2 Zertifikat auf einem Windows System installieren, auf dem die Windows-Agenten bereits installiert sind 106
4.3.3 Zertifikatsdateien auf einem Linux oder VMware System installieren 107
4.3.3.1 Zertifikatsdateien gemeinsam mit den ServerView Agenten installieren 107
4.3.3.2 Zertifikat auf einem Linux/VMware System installieren, auf dem die ServerView-Agenten bereits installiert sind . . . 109
4.3.4 Zertifikat via ServerView Update Manager installieren (auf einem Windows / Linux / VMware System) 110
4.3.4.1 Mit dem ServerView Update Manager das CMS-Zertifikat auf dem verwalteten Server installieren (Überblick) 111
4.3.4.2 CMS-Zertifikat auf dem verwalteten Server installieren . . . 115
4.3.4.3 CMS-Zertifikat auf dem verwalteten Server deinstallieren . . 115

5 Rollenbasierte Berechtigungen für den Zugriff auf den Operations Manager 117

5.1 Privilegien-Kategorien und zugehörige Berechtigungen . . 118
5.1.1 Privilegien-Kategorien (Überblick) 118
5.1.2 Kategorie AgentDeploy 119
5.1.3 Kategorie AlarmMgr 119
5.1.4 Kategorie ArchiveMgr 120
5.1.5 Kategorie BackupMgr 120
5.1.6 Kategorie Common 121
5.1.7 Kategorie ConfigMgr 122
5.1.8 Kategorie InvMgr 122
5.1.9 Kategorie iRMC_MMB 123
5.1.10 Kategorie PerfMgr 124

5.1.11 Kategorie PowerMon . . . 125
5.1.12 Kategorie RackManager . . . 125
5.1.13 Kategorie RaidMgr . . . 126
5.1.14 Kategorie RemDeploy . . . 126
5.1.15 Kategorie ReportMgr . . . 127
5.1.16 Kategorie SCS . . . 127
5.1.17 Kategorie ServerList . . . 128
5.1.18 Kategorie UpdMgr . . . 129
5.1.19 Kategorie UserMgr . . . 130
5.1.20 Kategorie VIOM . . . 130

5.2 In OpenDJ vordefinierte Benutzer und Rollen . . . 131

6 Audit-Logging . . . 135

6.1 Lage der Audit-Log-Information im Speicher . . . 136

6.2 Einträge des Audit-Logs . . . 137
6.2.1 Typen von Audit-Log-Einträgen . . . 138
6.2.2 Header eines Audit-Log-Eintrags . . . 139
6.2.3 Strukturierte Daten eines Audit-Log-Eintrags . . . 140
6.2.3.1 origin-Element . . . 140
6.2.3.2 ServerView:env@231-Element . . . 141
6.2.3.3 ServerView:audit@231-Element . . . 141
6.2.3.4 ServerView[.<COMP_NAME>]:msg@231-Element . . . 142
6.2.3.5 ServerView[.<COMP_NAME>]:<operation>@231-Element 142
6.2.4 Beispiele: Einträge in der Audit-Log-Datei . . . 146

7 Anhang 1 - Globale iRMC S2/S3-Benutzerverwaltung via Verzeichnisdienst . . . 149

7.1 Konzept der Benutzerverwaltung für den iRMC S2/S3 . . . 150

7.2 Globale Benutzerverwaltung für den iRMC S2/S3 . . . 152
7.2.1 Überblick . . . 153
7.2.2 iRMC S2/S3-Benutzerverwaltung mithilfe eines LDAP-Verzeichnisdienstes (Konzept) . . . 154
7.2.2.1 Globale iRMC S2/S3-Benutzerverwaltung über Berechtigungsgruppen und Rollen . . . 154
7.2.2.2 Organizational Unit (OU) SVS . . . 156
7.2.2.3 Server-übergreifende globale Benutzerberechtigungen . . . 158
7.2.2.4 SVS: Berechtigungsprofile werden über Rollen definiert . . . 160

7.2.3 SVS_LdapDeployer - Strukturen „SVS“ und „iRMCgroups“ generieren, pflegen und löschen . . . 162
7.2.3.1 Konfigurationsdatei (xml-Datei) . . . 162
7.2.3.2 SVS_LdapDeployer starten . . . 163
7.2.3.3 -deploy: LDAP-Struktur erzeugen oder ändern . . . 165
7.2.3.4 -delete: LDAP-Struktur löschen . . . 167
7.2.4 Typische Anwendungsszenarien . . . 168
7.2.4.1 Erst-Konfiguration einer LDAP v2-Struktur durchführen . . . 168
7.2.4.2 LDAP v2-Struktur neu generieren oder erweitern . . . 168
7.2.4.3 LDAP v2-Struktur neu generieren und Authentisierungsdaten anfordern und speichern . . . 169
7.2.5 iRMC S2/S3-Benutzerverwaltung via Microsoft Active Directory . . . 170
7.2.5.1 LDAP/SSL-Zugriff des iRMC S2/S3 am Active Directory Server konfigurieren . . . 171
7.2.5.2 iRMC S2/S3-Benutzer einer Rolle (Berechtigungsgruppe) zuordnen . . . 176
7.2.6 iRMC S2/S3-Benutzerverwaltung via Novell eDirectory . . . 183
7.2.6.1 Software-Komponenten und Systemanforderungen . . . 183
7.2.6.2 Novell eDirectory installieren . . . 184
7.2.6.3 Novell eDirectory konfigurieren . . . 191
7.2.6.4 iRMC S2/S3-Benutzerverwaltung in Novell eDirectory integrieren . . . 197
7.2.6.5 iRMC S2/S3-Benutzer der Berechtigungsgruppe zuordnen . 203
7.2.6.6 Tipps zur Administration von Novell eDirectory . . . 207
7.2.7 iRMC S2/S3-Benutzerverwaltung via OpenLDAP . . . 210
7.2.7.1 OpenLDAP installieren . . . 210
7.2.7.2 SSL-Zertifikate erzeugen . . . 210
7.2.7.3 OpenLDAP konfigurieren . . . 211
7.2.7.4 iRMC S2/S3-Benutzerverwaltung in OpenLDAP integrieren . 213
7.2.7.5 Tipps zur Administration von OpenLDAP . . . 217
7.2.8 E-Mail-Benachrichtigung an globale iRMC S2/S3-Benutzer konfigurieren . . . 219
7.2.8.1 Globale E-Mail-Benachrichtigung . . . 220
7.2.8.2 Benachrichtigungsgruppen (Alert Roles) anzeigen . . . 224
7.2.8.3 iRMC S2/S3-Benutzer einer Benachrichtigungsgruppe (Alert Role) zuordnen . . . 226
7.2.9 SSL Copyright . . . 227

8 Anhang 2 - Globale iRMC S4-Benutzerverwaltung via Verzeichnisdienst 229

8.1 Konzept der Benutzerverwaltung für den iRMC S4 230

8.2 Globale Benutzerverwaltung für den iRMC S4 232
8.2.1 Überblick 233
8.2.2 iRMC S4-Benutzerverwaltung mithilfe eines LDAP-Verzeichnisdienstes (Konzept) 234
8.2.2.1 Globale iRMC S4-Benutzerverwaltung über Berechtigungsgruppen und Rollen 234
8.2.2.2 Organizational Unit (OU) SVS 236
8.2.2.3 Server-übergreifende globale Benutzerberechtigungen . . . 238
8.2.2.4 SVS: Berechtigungsprofile werden über Rollen definiert . . 240
8.2.3 SVS_LdapDeployer - Struktur „SVS“ generieren, pflegen und löschen 242
8.2.3.1 Konfigurationsdatei (xml-Datei) 242
8.2.3.2 SVS_LdapDeployer starten 243
8.2.3.3 -deploy: LDAP-Struktur erzeugen oder ändern 245
8.2.3.4 -delete: LDAP-Struktur löschen 247
8.2.4 Typische Anwendungsszenarien 248
8.2.4.1 Erst-Konfiguration einer LDAP v2-Struktur durchführen . . . 248
8.2.4.2 LDAP v2-Struktur neu generieren oder erweitern 248
8.2.4.3 LDAP v2-Struktur neu generieren und Authentisierungsdaten anfordern und speichern 249
8.2.5 iRMC S4-Benutzerverwaltung via Microsoft Active Directory . 250
8.2.5.1 LDAP/SSL-Zugriff des iRMC S4 am Active Directory Server konfigurieren 251
8.2.5.2 iRMC S4-Benutzer einer Rolle (Berechtigungsgruppe) zuordnen 256
8.2.6 iRMC S4-Benutzerverwaltung via Novell eDirectory 263
8.2.6.1 Software-Komponenten und Systemanforderungen 263
8.2.6.2 Novell eDirectory installieren 264
8.2.6.3 Novell eDirectory konfigurieren 271
8.2.6.4 iRMC S4-Benutzerverwaltung in Novell eDirectory integrieren 277
8.2.6.5 iRMC S4-Benutzer der Berechtigungsgruppe zuordnen . . 283
8.2.6.6 Tipps zur Administration von Novell eDirectory 287
8.2.7 iRMC S4-Benutzerverwaltung via OpenLDAP 290
8.2.7.1 OpenLDAP installieren 290
8.2.7.2 SSL-Zertifikate erzeugen 290

8.2.7.3 OpenLDAP konfigurieren 291
8.2.7.4 iRMC S4-Benutzerverwaltung in OpenLDAP integrieren . . 293
8.2.7.5 Tipps zur Administration von OpenLDAP 297
8.2.8 E-Mail-Benachrichtigung an globale iRMC S4-Benutzer konfigurieren 299
8.2.8.1 Globale E-Mail-Benachrichtigung 300
8.2.8.2 Benachrichtigungsgruppen (Alert Roles) anzeigen 304
8.2.8.3 iRMC S4-Benutzer einer Benachrichtigungsgruppe (Alert Role) zuordnen 306
8.2.9 SSL Copyright 307

1 Einleitung

Dieses Handbuch beschreibt das Autorisierungs- und Authentifizierungskonzept, auf dem die globale Benutzerverwaltung und die Sicherheitsarchitektur der ServerView Suite und des RMC S2/S3/S4 basieren.

1.1 Autorisierungs- und Authentifizierungskonzept

Benutzerverwaltung und Sicherheitsarchitektur der ServerView Suite und des iRMC S2/S3/S4 basieren auf drei grundlegenden Konzepten:

– Globale Benutzerverwaltung mithilfe eines LDAP-Verzeichnisdienstes

– Rollenbasierte Zugangskontrolle (Role Based Access Control, RBAC)

– Single Sign-on (SSO) auf Basis eines Centralized Authentication Service (CAS)

Globale Benutzerverwaltung mithilfe eines LDAP-Verzeichnisdienstes

Benutzer werden mithilfe eines Verzeichnisdienstes zentral für alle angeschlossenen Management-Stationen (CMS) gespeichert und verwaltet. Der Verzeichnisdienst liefert alle für die Authentifizierung und Autorisierung von Benutzern erforderlichen Informationen.

Als Verzeichnisdienst verwenden Sie wahlweise den vorkonfigurierten Verzeichnisdienst (ForgeRock's OpenDJ) des ServerView Operations Managers oder einen bereits im Einsatz befindlichen, konfigurierten Verzeichnisdienst (wie z.B. Microsoft Active Directory).

Rollenbasierte Zugangskontrolle (Role Based Access Control, RBAC)

Rollenbasierte Zugangskontrolle (RBAC) steuert die Zugangkontrolle über einen Satz definierter Benutzerrollen. Jedem Benutzer werden dabei eine oder mehrere Rollen zugewiesen, wobei jeder Rolle wiederum eine oder mehrere Berechtigungen (Privilegien) zugewiesen sind.

Mit RBAC können Sie Ihr Sicherheitskonzept an der Organisationsstruktur Ihres Unternehmens ausrichten, indem Sie jeder Rolle ein aufgabenorientiertes Berechtigungsprofil zuordnen.

Im Verzeichnisdienst OpenDJ, der automatisch mit dem ServerView Operations Manager installiert wird, ist RBAC bereits implementiert. Sollten Sie jedoch bereits einen konfigurierten Verzeichnisdienst wie Active Directory verwenden, dann können Sie dort ergänzend die ServerView-spezifischen Berechtigungen (Privilegien) importieren. Danach können Sie die erforderlichen Rollen denjenigen Benutzern zuweisen, die über die damit verbundenen Berechtigungen verfügen sollen.

Single Sign-on (SSO)

Für die Anmeldung an den einzelnen ServerView-Komponenten unterstützt die ServerView Suite das Single Sign-on (SSO)-Login. SSO basiert auf einem zentralisierten Authentifizierungsservice, dem **C**entralized **A**uthentication **S**ervice (CAS). SSO bedeutet, dass Sie Ihre Authentizität nur einmal nachweisen müssen. Einmal erfolgreich authentifiziert, erhalten Sie Zugang zu allen ServerView-Komponenten, ohne sich bei einer dieser Komponenten neu anmelden zu müssen.

1.2 Zielgruppen und Zielsetzung des Handbuchs

Dieses Handbuch wendet sich an Systemadministratoren, Netzwerkadministratoren und Service-Techniker, die bereits über eine grundlegende Kenntnis der Hardware und Software verfügen. Das Handbuch gibt einen Überblick über das Autorisierungs- und Authentifizierungskonzept der ServerView Suite und beschreibt detailliert, wie Sie die ServerView-Benutzerverwaltung einrichten oder in die bereits bestehende Benutzerverwaltung Ihrer IT integrieren.

1.3 Struktur des Handbuchs

Das Handbuch liefert Informationen zu folgenden Themen:

- **Kapitel 2: Benutzerverwaltung und Sicherheitsarchitektur (Überblick)**

  Diese Kapitel gibt einen Überblick über das Autorisierungs- und Authentifizierungskonzept der ServerView Suite.

- **Kapitel 3: ServerView-Benutzerverwaltung mit LDAP-Verzeichnisdienst**

  Dieses Kapitel liefert Informationen zu folgenden Themen:

  – Zugang zum Verzeichnisdienst konfigurieren.

  – ServerView-Benutzerverwaltung mit OpenDJ

  – ServerView-Benutzerverwaltung in Microsoft Active Directory integrieren.

- **Kapitel 4: SSL-Zertifikate auf der zentralen Management-Station und den Managed Nodes verwalten**

  Dieses Kapitel liefert Informationen zu folgenden Themen:

  – SSL-Zertifikate verwalten (Überblick).

  – SSL-Zertifikaten auf der zentralen Management-Station verwalten.

  – Verwalteten Server Systeme für Role Based Access (RBAC) und Client-Authentifizierung einrichten.

- **Kapitel 5: Rollenbasierte Autorisierung für den Zugriff auf den Operations Manager**

  Dieses Kapitel liefert Informationen zu folgenden Themen:

  – Privilegien-Kategorien und zugehörige Berechtigungen (Privilegien)

  – Vordefinierte Benutzer und Rollen in OpenDJ

- **Kapitel 6: Audit-Logging**

  Dieses Kapitel liefert detaillierte Informationen zum CAS-spezifischen Audit-Logging, zur Lage des Audit-Log im Speicher sowie zur Struktur der Audit-Log-Einträge.

- **Anhang 1: Globale iRMC S2/S3 Benutzerverwaltung via Verzeichnisdienst**

  Dieses Kapitel liefert Informationen zu folgenden Themen:

  – Konzept der globalen Benutzerverwaltung für den iRMC S2/S3.

  – Benutzerberechtigungen, Berechtigungsgruppen und Rollen.

  – iRMC S2/S3-Benutzerverwaltung mit Microsoft Active Directory, Novell eDirectory, OpenLDAP und OpenDJ.

- **Anhang 2: Globale iRMC S4 Benutzerverwaltung via Verzeichnisdienst**

  Dieses Kapitel liefert Informationen zu folgenden Themen:

  – Konzept der globalen Benutzerverwaltung für den iRMC S4.

  – Benutzerberechtigungen, Berechtigungsgruppen und Rollen.

  – iRMC S4-Benutzerverwaltung mit Microsoft Active Directory, Novell eDirectory, OpenLDAP und OpenDJ.

1.4 Änderungen seit der vorherigen Ausgabe des Handbuchs

Diese Ausgabe des Handbuchs "Benutzerverwaltung in ServerView" ist gültig für die Version 6.30 des ServerView Operations Managers und löst das folgende Online-Handbuch ab: "ServerView Suite - Benutzerverwaltung in ServerView", Ausgabe Oktober 2013.

Das Handbuch bietet die folgenden Änderungen und Erweiterungen:

- Für die Änderung des Passworts des schreibgeschützten Benutzerkontos, das für LDAP-Abfragen unter Active Directory verwendet wird, wurde ein neues Skript bereitgestellt. Mit diesem Skript können Sie das Passwort ändern, ohne einen Windows-Service oder Linux-Dämon neu starten zu müssen, siehe Abschnitt "Passwort des LDAP-Bind-Kontos ändern" auf Seite 75.

1.5 ServerView Suite Link-Sammlung

Fujitsu Technology Solutions stellt Ihnen über die Link-Sammlung zahlreiche Downloads und weiterführende Informationen zur ServerView Suite und zu PRIMERGY Servern zur Verfügung.

Zur ServerView Suite werden Ihnen Links zu folgenden Themen angeboten:

- Forum
- Handbücher
- Service Desk
- Produktinformationen
- Schulungen
- Sicherheitsinformationen
- Software Downloads

Die Downloads umfassen u.a.:

- aktuelle Software-Stände zur ServerView Suite sowie ergänzende Readme-Dateien.
- Informationsdateien und Aktualisierungsdateien (Update Sets) für systemnahe Software-Komponenten (BIOS, Firmware, Treiber, ServerView-Agenten und ServerView-Update-Agenten) zur Aktualisierung der PRIMERGY Server anhand des ServerView Update Managers oder für den lokalen Update einzelner Server anhand des ServerView Update Managers Express.
- die aktuellen Versionen aller Dokumentationen zur ServerView Suite

Die Downloads können kostenlos vom Fujitsu Technology Solutions Web-Server heruntergeladen werden.

Zu PRIMERGY Servern werden Ihnen Links zu folgenden Themen angeboten:

- Ersatzteilkatalog
- Handbücher
- Service Desk
- Produktinformationen

Zugriff auf die ServerView Link-Sammlung

Die Link-Sammlung der ServerView Suite erreichen Sie über verschiedene Wege:

1. über den ServerView Operations Manager

   ► Wählen Sie auf der Startseite bzw. in der Menüzeile *Help – Links* aus.

   Anschließend wird die Startseite der Link-Sammlung angezeigt.

2. über die ServerView Suite DVD bzw. über die Startseite der Online-Dokumentation zur ServerView Suite auf dem Manual-Server von Fujitsu Technology Solutions

   Sie gelangen auf die Startseite der Online-Dokumentation mit folgendem Link:

   http://manuals.ts.fujitsu.com

   ► Wählen Sie links in der Auswahlliste *Industry standard servers* aus.

   ► Klicken Sie auf den Menüpunkt *PRIMERGY ServerView Links*.

   Anschließend wird die Startseite der ServerView Suite Link-Sammlung angezeigt.

3. über die ServerView Suite DVD

   ► Markieren Sie im Startfenster der ServerView Suite DVD die Option *ServerView Software Produktauswahl*.

   ► Klicken Sie auf *Starten*. Sie gelangen auf die Seite der Software Produkte der ServerView Suite.

   ► Wählen Sie in der Menüleiste *Links*.

   Anschließend wird die Startseite der ServerView Suite Link-Sammlung angezeigt.

1.6 Dokumentation zur ServerView Suite

Die Dokumentation ist über das Internet als Download kostenlos erhältlich. Die Online-Dokumentation zur ServerView Suite finden Sie unter *http://manuals.ts.fujitsu.com* und dem Link *x86 Servers*.

Einen Überblick über die Dokumentation, die Sie unter *ServerView Suite* finden, sowie die Ablagestruktur können Sie der ServerView Suite Sitemap (*ServerView Suite* - *Site Overview*) entnehmen.

1.7 Darstellungsmittel

In diesem Handbuch werden die folgenden Drstellungsmittel verwendet:

Achtung	Mit diesem Symbol wird auf Gefahren hingewiesen, die zu Gesundheitsgefährdung, Datenverlust und Geräteschäden führen können.
	Mit diesem Symbol werden wichtige Informationen und Tipps hervorgehoben.
►	Mit diesem Symbol wird ein Arbeitsschritt, den Sie ausführen müssen, dargestellt.
Kursive Schrift	Im Fließtext werden Kommandos, Menüpunkte, die Namen von Schaltflächen, Optionen, Dateinamen und Pfadnamen kursiv dargestellt.
`dicktengleich`	Ausgaben des Systems werden dicktengleich dargestellt.
`halbfett dicktengleich`	Befehle, die über die Tastatur eingegeben werden sollen, werden halbfett und dicktengleich dargestellt.
<abc>	Kennzeichnen optionale Eingaben.
Tastensymbole	Tasten werden entsprechend ihrer Abbildung auf der Tastatur dargestellt. Wenn explizit Großbuchstaben eingegeben werden sollen, so wird die Shift-Taste angegeben, z. B. SHIFT - A für A. Müssen zwei Tasten gleichzeitig gedrückt werden, wird dies durch einen Bindestrich zwischen den Tastensymbolen gekennzeichnet.

Tabelle 1: Darstellungsmittel

Wird auf Textstellen in diesem Handbuch verwiesen, so wird die Überschrift des Kapitels bzw. Abschnitts genannt, wobei sich die Seitenangabe auf den Beginn des Abschnitts bezieht.

Bildschirmabzüge

Beachten Sie, dass die Bildschirmausgabe teilweise vom verwendeten System abhängt und deshalb eventuell einige Details nicht exakt der Ausgabe entsprechen, die Sie auf Ihrem System sehen. Ebenso können bezüglich der verfügbaren Menüpunkte systembedingte Abweichungen auftreten.

2 Benutzerverwaltung und Sicherheitsarchitektur (Überblick)

Das in der Benutzerverwaltung und Sicherheitsarchitektur der ServerView Suite angebotene Autorisierungs- und Authentifizierungskonzept basiert auf drei wesentlichen Grundlagen:

– "Globale Benutzerverwaltung mit LDAP-Verzeichnisdienst" auf Seite 22:

  Benutzer werden mithilfe eines Verzeichnisdienstes zentral für alle angeschlossenen Management-Stationen gespeichert und verwaltet. Der Verzeichnisdienst liefert alle für die Authentifizierung und Autorisierung von Benutzern erforderlichen Informationen.

– "Rollenbasierte Zugangskontrolle (RBAC)" auf Seite 26:

  Rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC) regelt die Rechtevergabe über Benutzerrollen. Dabei definiert jede Rolle ein spezifisches, aufgabenorientiertes Berechtigungsprofil.

– "Single Sign-on (SSO) mithilfe eines CAS Service" auf Seite 29:

  Die verschiedenen ServerView Produkte haben ihre eigenen Web Server oder Applikations-Server, die alle die Identität jedes einzelnen Benutzers feststellen müssen, bevor sie den Zugang gestatten. Dadurch würde ein Benutzer bei jedem Wechsel vom Web GUI eines Produkt zum Web GUI eines anderen Produkts erneut zur Eingabe seiner Berechtigungsdaten aufgefordert.

  Beim Single Sign-on (SSO) meldet sich ein Benutzer einmal an und kann danach auf alle Systeme und Dienste der „SSO Domäne“ zugreifen, ohne sich dabei jedes Mal neu anmelden zu müssen. (Eine SSO-Domäne umfasst alle Systeme bei denen die Authentifizierung über denselben CAS Service abgewickelt wird).

Die folgenden Abschnitte gehen näher auf diese Konzepte ein.

Zusammenspiel zwischen ServerView Operations Manager ≥ 5.0 und ServerView Agenten < 5.0:

Die ServerView Agenten < V5.0 unterstützen die oben erwähnten Konzepte nicht. Trotzdem können Sie mit dem ServerView Operations Manager V5.x beliebige Operationen (einschließlich der sicherheitsrelevanten Operationen) auf den ServerView Agenten < V5.0 durchführen. Hierfür muss die Benutzer/Passwort-Liste des Operation Managers gültige Einträge (Benutzer/Passwort-Einträge mit den geeigneten Berechtigungen) für die betreffenden verwalteten Server (Managed Nodes) enthalten. Die Vorgehensweise ist ähnlich wie beim ServerView Operations Manger < 5.0. Single Sign-on wird jedoch nicht unterstützt.

2.1 Voraussetzungen

Benutzerverwaltung und Sicherheitsarchitektur der ServerView Suite setzen folgende Software voraus:

- JBoss Web Server

  Ab der Version 5.0 verwendet der ServerView Operations Manager den JBoss Web Server. Die benötigten Dateien werden automatisch mit der Software des ServerView Operations Manager installiert.

  JBoss wird als eigenständiger Dienst unter dem Namen *ServerView JBoss Applications Server 7* konfiguriert. Den Service können Sie wie folgt starten / stoppen:

  – Auf Windows Server 2008/2012 Systemen:

    Wählen Sie *Start – Administrative Tools – Services.*

    Alternativ können Sie auf allen Windows Systemen zum Starten und Stoppen des JBoss Service die folgenden CLI-Kommandos verenden:

    ```
    "%WINDIR%\system32\net.exe" start "ServerView JBoss
    Application Server 7"
    ```

    ```
    "%WINDIR%\system32\net.exe" start "ServerView JBoss
    Application Server 7"
    ```

  – Auf Linux Systemen über das folgende Kommando:

    ```
    /etc/init.d/sv_jboss start|stop
    ```

- LDAP Verzeichnisdienst

  Während der Installation des ServerView Operations Managers können Sie wählen, ob Sie den vom Operations Manager intern genutzten Verzeichnisdienst OpenDJ oder einen bereits vorhandenen Verzeichnisdienst (z.B. Microsoft Active Directory) nutzen wollen.

- Centralized Authentication Service (CAS)

  Der CAS Service wird für die Single Sign-on (SSO)-Funktionalität benötigt. Der CAS Service speichert Server-seitig die Berechtigungsdaten der Benutzer, um danach beim Aufruf der verschiedenen Dienste die Benutzer-Authentifizierung transparent durchzuführen.

  CAS wird bei der Installation der Operations Manager-Software automatisch mit installiert.

Einzelheiten zur Installation des ServerView Operations Managers, der die oben genannten Komponenten enthält, finden Sie im Handbuch "ServerView Operations Manager - Installation unter Windows“ und "ServerView Operations Manager - Installation unter Linux“.

2.2 Globale Benutzerverwaltung mit LDAP-Verzeichnisdienst

Die globale Benutzerverwaltung von ServerView Suite und iRMC S2/S3/S4 speichern die Benutzerkennungen für alle zentralen Management-Stationen (CMS) / iRMC S2/S3/S4 jeweils zentral im Verzeichnis eines LDAP-Verzeichnisdienstes. Auf diese Weise lassen sich die Benutzerkennungen auf einem zentralen Server verwalten. Die Benutzerkennungen können somit von allen CMS und iRMC S2/S3/S4 verwendet werden, die mit diesem Server im Netz verbunden sind.

Wichtiger Hinweis:

Die Abwicklung einer integrierten Benutzerverwaltung auf Basis eines gemeinsamen Verzeichnisdienstes funktioniert nur dann sowohl für ServerView-Benutzer als auch für iRMC S2/S3/S4-Benutzer, wenn der betreffende iRMC S2/S3/S4 als Mitglied des Departments *DEFAULT* konfiguriert ist.

In diesem Handbuch wird der Begriff "Benutzerverwaltung des iRMC S2/S3/S4" im Sinne von "globaler" iRMC S2/S3/S4-Benutzerverwaltung verwendet. Darüber hinaus unterstützt der iRMC S2/S3/S4 eine "lokale" Benutzerverwaltung. Bei der lokalen Benutzerverwaltung sind die zugehörigen Benutzerkennungen lokal im nicht-flüchtigen Speicher des iRMC S2/S3/S4 abgelegt und werden über die iRMC S2/S3-Benutzerschnittstellen verwaltet. Zu Einzelheiten siehe Handbücher "iRMC S2/S3 - integrated Remote Management Controller" und "iRMC S4 - integrated Remote Management Controller".

2.2.1 Vorteile durch Verwendung eines Verzeichnisdienstes

Die Verwendung eines Verzeichnisdienstes bietet folgende Vorteile:

– Ein Verzeichnisdienst verwaltet "reale" Benutzeridentitäten und gestattet so die Verwendung von persönlichen Identifikationsdaten anstelle von unspezifischen Benutzerkonten.

– Ein Verzeichnisdienst entkoppelt die Benutzerverwaltung vom Server Management. Ein Server-Administrator kann somit Benutzerrechte nur dann ändern, wenn er zum Ändern von Daten des Verzeichnisdienstes befugt ist.

ServerView verwendet den Verzeichnisdienst sowohl für Benutzer-Authentifizierung als auch Benutzer-Autorisierung:

– Authentifizierung prüft die Identität des Benutzers: "**Wer** sind Sie?"

– Autorisierung definiert die Rechte des Benutzers: "**Was** dürfen Sie tun?"

Der Einsatz eines Verzeichnisdienstes für die Management-Station (Central Management Station, CMS) ermöglicht es darüber hinaus, für das Anmelden an der CMS dieselben Kennungen zu verwenden wie für das Anmelden an den verwalteten Servern.

2.2.2 Unterstützte Verzeichnisdienste

Von der ServerView Suite unterstützte Verzeichnisdienste:

Derzeit unterstützt die ServerView Suite folgende Verzeichnisdienste:

– OpenDJ (ausgeführt im "embedded" Modus unter JBoss)
– Microsoft Active Directory

Während der Installation des ServerView Operations Managers können Sie den ServerView-internen Verzeichnisdienst (OpenDJ) wählen.

Vom iRMC S2/S3/S4 unterstützte Verzeichnisdienste:

Derzeit unterstützt der iRMC S2/S3/S4 folgende Verzeichnisdienste:

– Microsoft Active Directory
– Novell eDirectory
– OpenLDAP
– OpenDJ (ausgeführt im "embedded" Modus unter JBoss)

2.2.3 Open DS oder einen bereits vorhandenen, konfigurierten Verzeichnisdienst verwenden

OpenDJ verwenden

Falls Sie bei der Installation des Operations Managers keinen separaten Verzeichnisdienst festlegen, installiert der Installation Wizard automatisch ForgeRock's OpenDJ als Verzeichnisdienst. Der Verzeichnisdienst läuft im "embedded Mode" unter JBoss. Somit ist OpenDJ nur dann verfügbar, wenn der Dienst *ServerView JBoss Application Server 7* ausgeführt wird.

Bereits existierenden, konfigurierten Verzeichnisdienst verwenden

Falls für die Benutzerverwaltung Ihrer IT-Umgebung bereits ein Verzeichnisdienst (z.B. Microsoft Active Directory) eingerichtet ist, können Sie diesen anstelle von OpenDJ verwenden.

2.2.4 Gemeinsame Benutzerverwaltung für ServerView Suite und iRMC S2/S3/S4

Sie können eine Server-übergreifende Benutzerverwaltung einrichten, die alle von der ServerView Suite verwalteten Server sowie die zugehörigen iRMC S2/S3/S4 gleichermaßen umfasst.

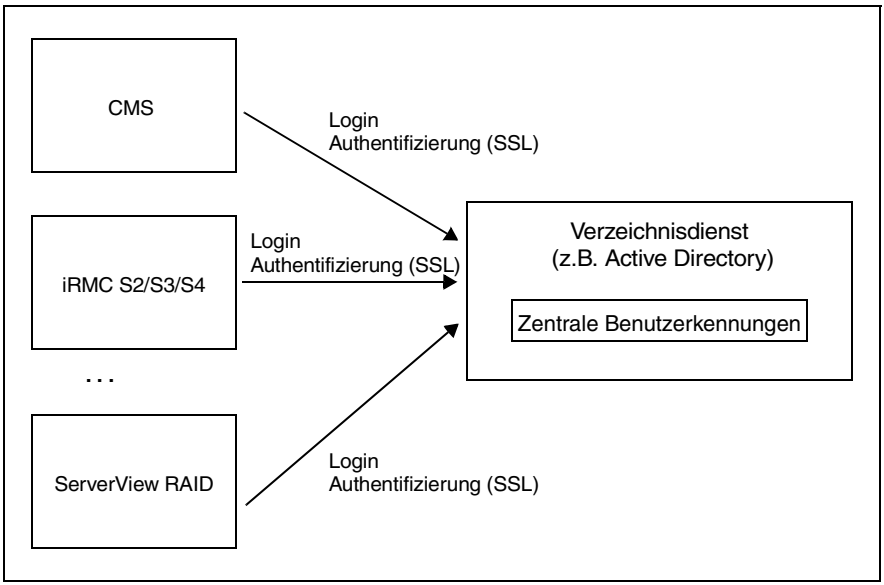


Bild 1: Gemeinsame Nutzung der globalen Benutzerkennungen durch die verschiedenen Komponenten der ServerView Suite.

Die Kommunikation zwischen den einzelnen Management-Stationen / iRMC S2/S3/S4 / ... und dem zentralen Verzeichnisdienst wird über das TCP/IP-Protokoll LDAP (**Li**ghtweight **D**irectory **A**ccess **P**rotocol) abgewickelt. LDAP ermöglicht den Zugriff auf die gängigsten zur Benutzerverwaltung geeigneten Verzeichnisdienste.

Aus Sicherheitsgründen wird dringend empfohlen, die Kommunikation über LDAP durch SSL abzusichern. Andernfalls werden Passwörter im Klartext übertragen.

2.3 Rollenbasierte Zugangskontrolle (RBAC)

Sowohl die Benutzerverwaltung der ServerView Suite als auch die globale iRMC S2/S3/S4-Benutzerverwaltung basieren auf der rollen-basierten Zugangskontrolle (Role-based access control, RBAC), mit der Sie Ihr Sicherheitskonzept an die Struktur Ihres Unternehmens anpassen können.

RBAC basiert auf dem Prinzip der minimalen Berechtigung. Demzufolge sollte kein Benutzer über mehr Berechtigungen (Privilegien) verfügen, als für die Benutzung einer bestimmten ServerView-Komponente oder zur Ausführung einer ServerView-spezifischen Aufgabe erforderlich sind.

2.3.1 Benutzer, Benutzerrollen und Berechtigungen (Privilegien)

RBAC regelt die Zuteilung von Berechtigungen an Benutzer über Benutzerrollen, anstatt die entsprechenden Berechtigungen den Benutzern direkt zuzuweisen:

– Jeder Benutzerrolle wird ein Satz von Berechtigungen zugeordnet. Jeder einzelne Satz definiert ein spezifisches, aufgabenorientiertes Berechtigungsprofil für Tätigkeiten an der ServerView Suite.

– Jedem Benutzer werden eine oder mehrere Rollen zugewiesen.

Das Konzept der Benutzerrollen bietet u.a folgende wesentlichen Vorteile:

– Die einzelnen Berechtigungen müssen nicht jedem Benutzer oder jeder Benutzergruppe separat zugewiesen werden. Stattdessen werden Berechtigungen der Benutzerrolle zugewiesen.

– Wenn sich die Berechtigungsstruktur ändert, müssen nur die in der Benutzerrolle enthaltenen Berechtigungen angepasst werden.

Jedem Benutzer können mehrere Rollen zugewiesen werden. In diesem Fall definieren sich die Berechtigungen eines Benutzers über die Summe der Berechtigungen aus allen Rollen, die diesem Benutzer zugewiesen sind.

2.3.2 RBAC-Implementierung in OpenDJ

RBAC ist bereits im Verzeichnisdienst OpenDJ implementiert, der bei der Installation des ServerView Operations Managers automatisch installiert wird.

Vordefinierte Benutzer und Rollen

Per Voreinstellung bietet OpenDJ die vordefinierten Benutzerrollen *Administrator*, *Monitor*, *Operator* und *UserAdministrator* an, die jeweils einem der vordefinierten Benutzer *Administrator*, *Monitor*, *Operator* bzw. *UserManager* fest zugeordnet sind. Durch Erzeugen zusätzlicher Benutzer, Rollen und Rollen-Benutzer-Zuordnungen können Sie Ihr Sicherheitskonzept auf Ihre Unternehmensstruktur ausrichten.

Bild 2 zeigt das Konzept der Rollen-basierten Zuweisung von Benutzerberechtigungen mit den Benutzernamen *Administrator*, *Monitor*, *Operator* und *UserManager* sowie den zugehörigen Rollen *Administrator*, *Monitor*, *Operator* und *UserAdministrator*.

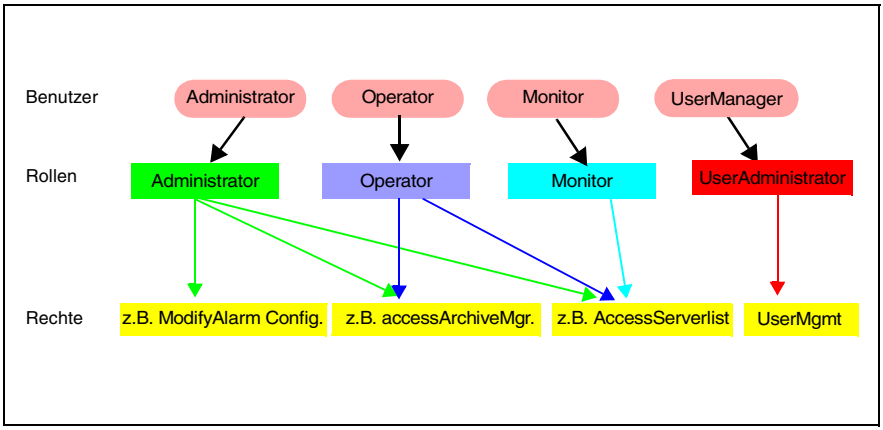


Bild 2: Beispiel für rollenbasierten Zuteilung von Benutzerberechtigungen

Genau genommen gibt es in OpenDJ noch zwei weitere vordefinierte Benutzerkennungen, die umfassend autorisiert und für spezielle Aufgaben reserviert sind: "cn=Directory Manager" (Directory Manager-Kennung von OpenDJ) und *svuser* (für den Zugriff auf den Verzeichnisdienst durch CAS und den Sicherheitsmodul von ServerView).

Der Umfang der durch die einzelnen Benutzerrollen erteilten Berechtigungen nimmt beginnend bei Monitor (niedrigste Berechtigungsstufe) über Operator bis Administrator (höchste Berechtigungsstufe) stetig zu. Näheres hierzu finden Sie Kapitel "Audit-Logging" auf Seite 135.

Die Rolle *UserAdministrator* fügt sich nicht in diese Hierarchie ein, da ihr Zweck lediglich darin besteht, die Privilegien für die Benutzverwaltung mit OpenDJ bereitzustellen. Wenn für die Benutzerverwaltung in ServerView ein externer Verzeichnisdienst (z.B. Active Directory) verwendet wird, wird die Rolle *UserAdministrator* nicht in diesen Verzeichnisdienst importiert.

Sicherheitskonzept an die Struktur Ihrer Organisation anpassen

Zur Ausrichtung Ihres Sicherheitskonzepts an Ihrer Unternehmensstruktur ermöglicht Ihnen die ServerView Suite, auf komfortable Weise zusätzliche Benutzer, Rollen und Rollen-Benutzer-Zuordnungen zu definieren, indem Sie den *User Management*-Link unterhalb des *Security*-Eintrags in der Startseite des ServerView Operations Managers Start-Seite benutzen.

2.3.3 RBAC bei einem bereits existierenden konfigurierten Verzeichnisdienst

Sie können die RBAC Benutzerverwaltung für ServerView auch in eine bereits existierende Benutzerverwaltung auf Basis eines konfigurierten Verzeichnisdienstes (z.B. Microsoft Active Directory) integrieren. Näheres hierzu finden Sie im Abschnitt "ServerView-Benutzerverwaltung in Microsoft Active Directory integrieren" auf Seite 65.

2.4 Single Sign-on (SSO) mithilfe eines CAS Service

Für die Benutzeranmeldung an den einzelnen Diensten (Web-Diensten) unterstützt die ServerView Suite die Single Sign-on (SSO)-Funktionalität. ServerView implementiert den SSO-Mechanismus mithilfe eines Centralized Authentication Service (CAS), der den SSO-Vorgang aus der Sicht des Benutzers völlig transparent abwickelt.

Achtung!

Melden Sie sich immer ab und schließen Sie Ihren Browser, bevor Sie Ihren PC unbeaufsichtigt lassen!

CAS speichert die Information über die Identität eines Benutzers in einem sicheren Browser-Cookie (Ticket Granting Cookie, TGC, siehe Seite 31), das automatisch gelöscht wird, wenn der Benutzer sich explizit abmeldet oder den Browser schließt. Eine unbeaufsichtigte Browser-Sitzung stellt deshalb eine ernste Sicherheitslücke dar.

Voraussetzung für die Nutzung von SSO:

– Der CAS-Service muss für alle iRMC S2/S3/S4 der SSO-Domäne konfiguriert sein (zu Einzelheiten siehe Handbücher "iRMC S2/S3 - integrated Remote Management Controller" und "iRMC S4 - integrated Remote Management Controller").

– Alle Systeme, die zur SSO-Domäne gehören, müssen die zentrale Management-Station (CMS) unbedingt über dieselbe Adressstruktur referenzieren. (Eine SSO-Domäne umfasst alle Systeme, deren Authentifizierung über denselben CAS-Service erfolgt.) Wenn Sie also z. B. den ServerView Operations Manager unter der Bezeichnung „my-cms.my-domain“ installiert haben, müssen Sie zur Konfiguration des CAS-Services für einen iRMC S2/S3/S4 genau dieselbe Bezeichnung angeben. Geben Sie dagegen nur „my-cms“ oder eine andere IP-Adresse von my-cms an, dann wird die SSO-Funktionalität zwischen den beiden Systemen nicht aktiviert.

2.4.1 CAS-basierte SSO-Architektur

Eine SSO-Architektur basiert auf den folgenden Komponenten und Elementen:

– CAS Service, der die zentralisierte Authentifizierung realisiert

– CAS Client als Komponente jeder CAS-fähigen ServerView Suite-Komponente

– Service Ticket (ST)

– Ticket Granting Ticket (TGT)

Der CAS Service steuert die zentrale Benutzer-Authentifizierung

Der CAS Service steuert die zentrale Benutzer-Authentifizierung. Hierfür vermittelt der CAS Service zwischen dem Browser auf der Management-Konsole und dem Verzeichnisdienst, der die Benutzer verwaltet.

Der CAS Client fängt Service-Anforderungen ab und leitet sie um

Der CAS Client ist Bestandteil jeder CAS-fähigen ServerView Suite-Komponente. Er fungiert als Filter, der jede Benutzeranforderung an eine ServerView Suite-Komponente abfängt und direkt zur Benutzer-Authentifizierung an den CAS Service weiterleitet. Der CAS Client leitet den Request an den CAS Service weiter, der anschließend die Benutzer-Authentifizierung durchführt.

Service Ticket (ST) und Ticket Granting Ticket (TGT)

Nach erfolgreicher Authentifizierung eines Benutzers weist der CAS Service dem Benutzer ein so genanntes Ticket Granting Ticket (TGT) zu. Technisch erfolgt dies durch Setzen eines entsprechenden sicheren Browser Cookies. Jedesmal, wenn der CAS Client einer ServerView Suite-Komponente einen HTTPS-Request zum CAS Service umleitet, veranlasst das TGT Cookie den CAS Service, ein Request-spezifisches Service Ticket (ST) zu erzeugen und, ergänzt um einen zusätzlichen Request-Parameter, an den CAS Client zurückzusenden. Daraufhin validiert der CAS Client das ST per Direktaufruf an den CAS Service und leitet den Request nur bei erfolgreicher Validierung an die ServerView Suite-Komponente weiter.

Ticket Granting Cookie (TGC)

Nach dem Aufbau einer SSO Sitzung mit dem CAS Service präsentiert der Web Browser dem CAS Service ein sicheres Cookie. Dieses Cookie enthält einen String zur Identifizierung eines Ticket Granting Ticket (TGT) und wird demzufolge als Ticket Granting Cookie (TGT Cookie oder TGC) bezeichnet.

Das TGT wird gelöscht, sobald der Benutzer sich beim CAS Service abmeldet oder den Web Browser schließt. Die Lebensdauer des Ticket Granting Ticket Cookie (TGT) ist in der Konfigurationsdatei des CAS Service festgelegt. Die maximale Lebensdauer des TGT beträgt maximal 24 Stunden. Dies bedeutet, dass ein Benutzer spätestens nach 24 Stunden abgemeldet wird. In einem installierten System kann die maximale Zeitspanne nicht verändert werden.

Wie CAS-basiertes SSO einen initialen SSO Request verarbeitet

Bild 3 veranschaulicht, wie CAS-basiertes Single Sign-on (SSO) eine initiale Single Sign-on-Authentifizierung durchführt.

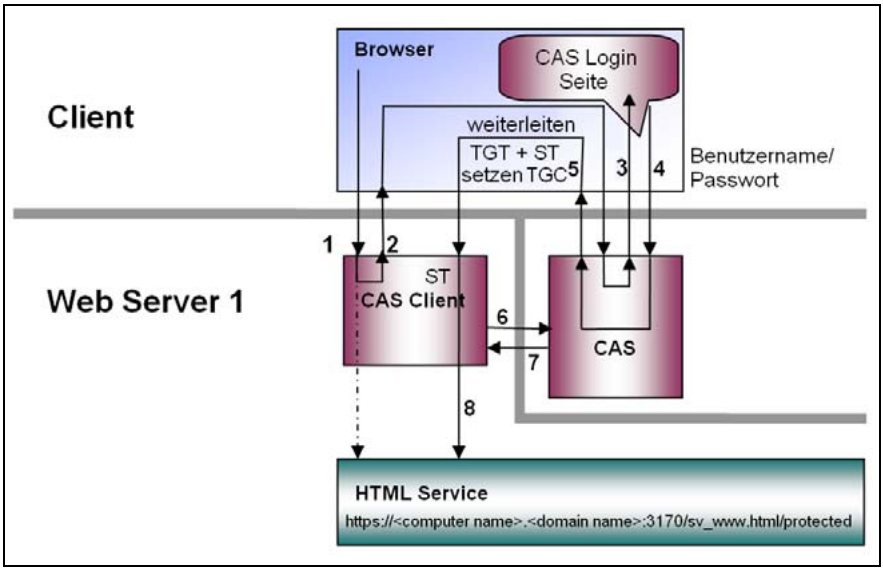


Bild 3: SSO Architektur mit CAS Service

Bedeutung:

1. Ein Benutzer ruft eine Komponente der ServerView Suite (z.B. ServerView Operations Manager) auf, indem er die URL der Komponente an der Management-Konsole eingibt.
2. Der Benutzer-Request wird an den CAS Service weitergeleitet.
3. Der CAS Service erzeugt ein CAS Anmeldefenster, das an der Management-Konsole angezeigt wird. Das CAS Anmeldefenster fordert den Benutzer auf, seine Berechtigungsdaten (Benutzername und Passwort) einzugeben.
4. Der Benutzer gibt seine Berechtigungsdaten ein.
5. Der CAS Service prüft Benutzername und Passwort und leitet den Request an die ursprünglich angeforderte ServerView-Komponente weiter. Außerdem setzt der CAS Service das TGT Cookie und weist dem Benutzer das Service Ticket (ST) und das Ticket Granting Ticket (TGT) zu.
6. Der CAS Client sendet das Service Ticket zur überprüfung an den CAS Service.
7. Nach erfolgreicher Validierung liefert der CAS Service die folgende Information zurück: "Service Ticket is ok.", <Benutzername>.
8. Die Web-Anwendung (ServerView-Komponente) beantwortet den ursprünglichen Request (siehe Schritt 1).

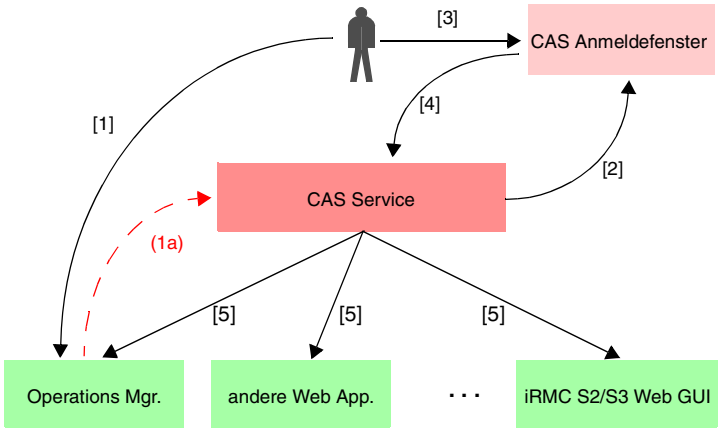
Wie CAS-basiertes SSO nachfolgende SSO Requests verarbeitet

Einmal erfolgreich für den Zugriff auf eine ServerView-Komponente (z.B. Operations Manager) authentifiziert, kann ein Benutzer eine andere Komponente (z.B. iRMC S2/S3/S4 Web-Oberfläche) aufrufen, ohne dass er noch einmal seine Berechtigungsdaten eingeben muss. In diesem Fall führt den CAS Service die Authentifizierung mithilfe des Ticket Granting Cookie (TGC) durch, das während eines früheren Anmeldevorgangs für diesen Benutzer gesetzt wurde.

Sofern das TGC einem gültigen Ticket Granting Ticket (TGT) entspricht, stellt der CAS Service jedesmal automatisch ein Service Ticket (ST) aus, wenn der Web-Browser den Dienst der einer Komponente der "SSO-Domäne" anfordert. Auf diese Weise hat der Benutzer Zugriff auf eine ServerView-Komponente, ohne dass er zur Eingabe seiner Berechtigungsdaten aufgefordert wird.

2.4.2 Single Sign-on aus Sicht des Benutzers

SSO bedeutet, dass Sie Ihre Authentizität nur einmal, nämlich beim CAS Service nachweisen müssen: Bei Ihrer ersten Anmeldung bei einer ServerView-Komponente (z.B. Operations Manager) zeigt der CAS Service ein eigenes Fenster, das Sie zur Eingabe Ihrer Berechtigungsdaten (Benutzername und Passwort) auffordert. Bei erfolgreicher Authentifizierung können Sie anschließend auf alle ServerView-Komponenten und iRMC S2/S3/S4 der SSO Domäne zugreifen, ohne sich erneut anmelden zu müssen.



(1) Ein Benutzer sendet einen HTTP-Request an eine ServerView-Komponente. (z.B. Operations Manager).

(1a) Unsichtbar für den Benutzer leitet CAS den Request intern an den CAS Service weiter.

(2) In seinem Anmeldefenster fordert der CAS Service den Benutzer zur Eingabe seiner Berechtigungsdaten auf.

(3) Der Benutzer gibt seine Benutzername / Passwort-Kombination ein und bestätigt.

(4) The CAS Service authentifiziert den Benutzer.

(5) Nach einmaliger erfolgreicher Authentifizierung hat der Benutzer Zugang zu jeder beliebigen Komponente , ohne erneut zur Anmeldung aufgefordert zu werden.

Bild 4: Single Sign-on-Prozedur aus Sicht des Benutzers

3 ServerView-Benutzerverwaltung mit LDAP-Verzeichnisdienst

Dieses Kapitel informiert über folgende Themen:

– "Zugang zum Verzeichnisdienst konfigurieren" auf Seite 35

– "ServerView-Benutzerverwaltung mit OpenDJ" auf Seite 36

– "ServerView-Benutzerverwaltung in Microsoft Active Directory integrieren" auf Seite 65

Wichtiger Hinweis:

Damit ServerView Benutzerverwaltung und globale iRMC S2/S3/S4-Benutzerverwaltung innerhalb derselben Organizational Unit (OU) *SVS* ausgeführt werden können, darf die iRMC S2/S3/S4-Benutzerverwaltung ausschließlich das Department *DEFAULT* verwenden.

Benachrichtigungsgruppen (Alert Roles) können in der ServerView Suite nicht verwendet werden, d.h. sie werden von allen ServerView-Komponenten mit Ausnahme des iRMC S2/S3/S4 ignoriert.

3.1 Zugang zum Verzeichnisdienst konfigurieren

Sowohl die zentralisierte Authentifizierung als auch die rollenbasierte Autorisierung der ServerView-Benutzerverwaltung stützen sich auf Daten, die zentral mithilfe eines Verzeichnisdienstes verwaltet werden. Die für den Verbindungsaufbau zu einem LDAP-Verzeichnisdienst benötigte Information wird während der Installation des Operations Managers angefordert.

Wenn Sie diese Einstellungen nachträglich ändern wollen, gehen Sie wie folgt vor:

– Wiederholen Sie auf Windows Systemen die Installation als Upgrade/Update-Installation.

– Führen auf Linux Systemen das folgende Kommando aus:
/opt/fujitsu/ServerViewSuite/svom/ServerView/Tools/ChangeComputerDetails.sh

3.2 ServerView-Benutzerverwaltung mit OpenDJ

Falls Sie bei der Installation des Operations Managers keinen separaten Verzeichnisdienst festlegen, installiert der Installation Wizard automatisch ForgeRock's OpenDJ als Verzeichnisdienst. Der Verzeichnisdienst läuft im "embedded Mode" unter JBoss. Somit ist OpenDJ nur dann verfügbar, wenn der Service *ServerView JBoss Application Server 7* ausgeführt wird.

3.2.1 Vordefinierte Benutzer und Rollen

Role Based Access Control (RBAC) ist im Verzeichnisdienst OpenDJ bereits implementiert. In OpenDJ sind die Benutzerrollen *Administrator*, *Monitor*, *Operator* und *UserAdministrator* vordefiniert, die jeweils genau einem der vordefinierten Benutzernamen *Administrator*, *Operator, Monitor* und *UserManager* zugeordnet sind. Für spezielle Aufgaben sind in OpenDJ zwei zusätzliche Benutzer definiert, die mit umfassenden Berechtigungen ausgestattet sind.

Tabelle 2 auf Seite 37 gibt einen Überblick über die in OpenDJ vordefinierten Benutzernamen, Passwörter und Rollen.

ACHTUNG!

Aus Sicherheitsgründen wird dringend empfohlen, die vordefinierten Passwörter baldmöglichst zu ändern. Einzelheiten zum Ändern von Passwörtern finden Sie im Abschnitt "Passwörter der vordefinierten Benutzer definieren/ändern" auf Seite 38.

Detaillierte Informationen zum Berechtigungsumfang, der durch die einzelnen Benutzerrollen gewährt wird, finden Sie im Kapitel "Rollenbasierte Berechtigungen für den Zugriff auf den Operations Manager" auf Seite 117.

Benutzername	Passwort	Benutzerrolle	LDAP Distinguished name / Beschreibung
./.	admin		cn=Directory Manager,cn=Root DNS, cn=config Kennung des OpenDJ Directory Managers. Ein Root DN (oder Root-Benutzer) kann generell auf alle Daten im Server zugreifen. In OpenDJ sind Root-Benutzer standardmäßig berechtigt, die Zugriffsüberprüfung zu umgehen. Root-Benutzer verfügen über die vollständige Berechtigung für Server-Konfiguration und Ausführung der meisten anderen Operationen. OpenDJ gestattet es, den Server mit mehren Root-Benutzern zu konfigurieren. Alle den Root-Benutzern gewährten Berechtigungen werden direkt über Privilegien erteilt.
svuser	Das Password muss während der Installation des Operations Managers angegeben werden.		cn=svuser,ou=users,dc=fujitsu,dc=com Diese Kennung wird verwendet für den Zugriff auf den Verzeichnisdienst durch CAS und den Sicherheitsmodul von ServerView. Die zugehörigen Daten finden Sie somit in derKonfigurationsdatei *<ServerView directory>\jboss\standalone\svconf\sv-sec-config.xml*.
Administrator	admin	Administrator	cn=ServerView Administrator,ou=users, dc=fujitsu,dc=com Standard-Benutzer für Administrator-Rolle.
Monitor	admin	Monitor	cn=ServerView Monitor,ou=users, dc=fujitsu,dc=com Standard-Benutzer für Monitor-Rolle.
Operator	admin	Operator	cn=ServerView Operator,ou=users, dc=fujitsu,dc=com Standard-Benutzer für Operator-Rolle.

Tabelle 2: In OpenDJ vordefinierte Benutzernamen, Rollen und Passwörter

Benutzername	Passwort	Benutzerrolle	LDAP Distinguished name / Beschreibung
UserManager	admin	UserAdministrator	cn=ServerView UserManager,ou=users, dc=fujitsu,dc=com Standard-Benutzer für UserAdministrator-Rolle.

Tabelle 2: In OpenDJ vordefinierte Benutzernamen, Rollen und Passwörter

3.2.2 Passwörter der vordefinierten Benutzer definieren/ändern

Wichtiger Hinweis:

Verwenden Sie innerhalb Ihrer Passwörter keinen Gegenschrägstrich (Backslash, "\").

3.2.2.1 Passwort des OpenDJ Directory Managers

Beachten Sie:

Das vordefinierte Passwort für den OpenDJ Directory Manager lautet "admin". Aus Sicherheitsgründen wird dringend empfohlen, die vordefinierten Passwörter baldmöglichst zu ändern.

In der nachfolgenden Erläuterung steht die Zeichenfolge "neu_dm_pw" als Platzhalter für das neue Passwort. Ersetzen Sie den Platzhalter durch ein geeignetes Passwort Ihrer Wahl.

Vordefiniertes Passwort des OpenDJ Directory Managers auf Windows Systemen ändern.

Beachten Sie:

Für die Einrichtung eines Passworts, das ein oder mehrere Prozent-Zeichen ("%") enthält, müssen Sie bei der Angabe des Passworts in der Kommandozeile jedes Prozent-Zeichen doppelt angeben. Um z.B. das Passwort `hello%world` einzurichten, müssen Sie in der Kommandozeile `hello%%world` eintippen.

Auf Windows Systemen ändern Sie das vordefinierte Passwort wie folgt:

1. Öffnen Sie eine Windows Eingabeaufforderung.
2. Stellen Sie sicher, dass die Umgebungsvariablen `JAVA_HOME` und `OPENDS_JAVA_HOME` auf das Installationsverzeichnis der Java Laufzeitumgebung (Java Runtime Environment, JRE) gesetzt sind. Falls das JRE z.B. unter *C:\Program Files (x86)\Java\jre7* installiert ist, setzen Sie die Umgebungsvariablen mit den folgenden Kommandos:

   ```
   SET JAVA_HOME=C:\Programme (x86)\Java\jre7

   SET OPENDS_JAVA_HOME=C:\Programme (x86)\Java\jre7

   SET PATH=C:\Program Files (x86)\Java\jre7\bin
   ```

3. Wechseln Sie in das Verzeichnis <*ServerView directory*>*opends\bat*.
4. Ändern Sie das Passwort des OpenDJ Directory Managers, indem Sie das folgende Kommando innerhalb einer einzigen Zeile eingeben:

   ```
   ldappasswordmodify -h localhost -p 1473
   -D "cn=Directory Manager" -w admin
   -a "dn:cn=Directory Manager,cn=Root DNs,cn=config"
   -n "new_dm_pw" -c "admin"
   ```

5. Starten Sie den Dienst *ServerView JBoss Application Server 7* neu, um Ihre Passwort-Einstellungen zu aktivieren.

Vordefiniertes Passwort des OpenDJ Directory Managers auf Linux Systemen ändern.

Beachten Sie:

Für die Einrichtung eines Passworts, das ein oder mehrere Sonderzeichen der Shell enthält, müssen Sie bei der Angabe des Passworts in der Kommandozeile jedes Sonderzeichen durch einen vorangestellten Backslash ("\") entwerten. Z.B. müssen Sie in der Kommandozeile `hello\$world` eintippen, um das Passwort `hello$world` einzurichten.

Auf Linux Systemen ändern Sie das vordefinierte Passwort wie folgt:

1. Öffnen Sie eine Kommando-Shell.
2. Stellen Sie sicher, dass die Umgebungsvariablen `JAVA_HOME` und `OPENDS_JAVA_HOME` auf das Installationsverzeichnis der Java Laufzeitumgebung (Java Runtime Environment, JRE) gesetzt sind. Falls das JRE z.B. unter *usr/java/default* installiert ist, setzen Sie die Umgebungsvariablen mit den folgenden Kommandos:

   ```
   export JAVA_HOME=/usr/java/default
   ```

   ```
   export OPENDS_JAVA_HOME=/usr/java/default
   ```

3. Wechseln Sie in das Verzeichnis */opt/fujitsu/ServerViewSuite/opends/bin*.
4. Ändern Sie das Passwort des OpenDJ Directory Managers, indem Sie das folgende Kommando innerhalb einer einzigen Zeile eingeben:

   ```
   ./ldappasswordmodify -h localhost -p 1473
   -D "cn=Directory Manager" -w admin
   -a "dn:cn=Directory Manager,cn=Root DNs,cn=config"
   -n "new_dm_pw" -c "admin"
   ```

5. Starten Sie den ServerView JBoss-Service neu, um Ihre Passwort-Einstellungen zu aktivieren:

   ```
   /etc/init.d/sv_jboss restart
   ```

3.2.2.2 Passwort von svuser definieren / ändern.

Der administrative Benutzer *svuser* wird in der Datenbank von OpenDJ während der Installation des ServerView Operations Managers erzeugt.

In früheren Versionen wurde *svuser* immer mit dem voreingestellten Passwort *admin* erzeugt. Ab Operations Manager V5.50 können Sie das Passwort für den Benutzer *svuser* während einer Dialog-basierten Installation angeben.

Zu Einzelheiten der Installation des Operations Managers siehe die Handbücher "Installation ServerView Operations Manager Software unter Windows" und "Installation ServerView Operations Manager Software unter Linux".

Das Passwort für *svuser* darf keine leere Zeichenkette sein.

Passwort von svuser auf Windows Systemen definieren / ändern

Erstmals **definieren Sie das Passwort** von *svuser* während der Installation des Operations Managers:

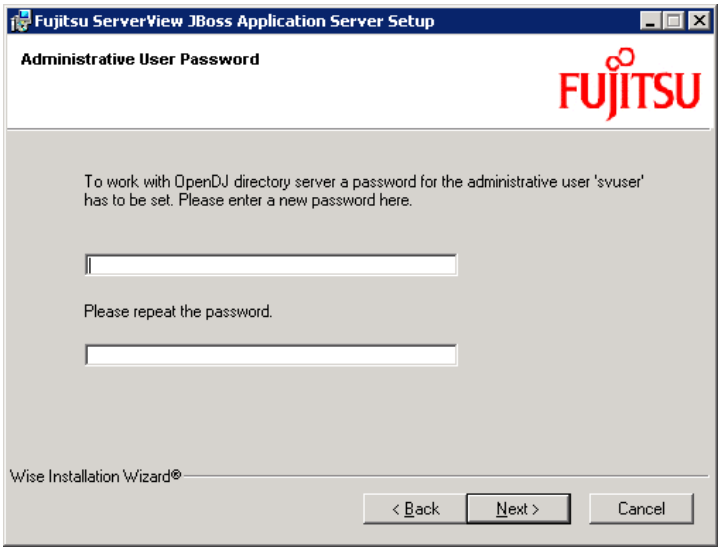

Fujitsu ServerView JBoss Application Server Setup
Administrative User Password
FUJITSU
To work with OpenDJ directory server a password for the administrative user 'svuser' has to be set. Please enter a new password here.
Please repeat the password.
Wise Installation Wizard®
< Back
Next >
Cancel

Bild 5: Passwort von svuser erstmals definieren (Windows)

Ändern können Sie das Passwort von *svuser* während einer Update/Upgrade-Installation des ServerView Operations Managers:

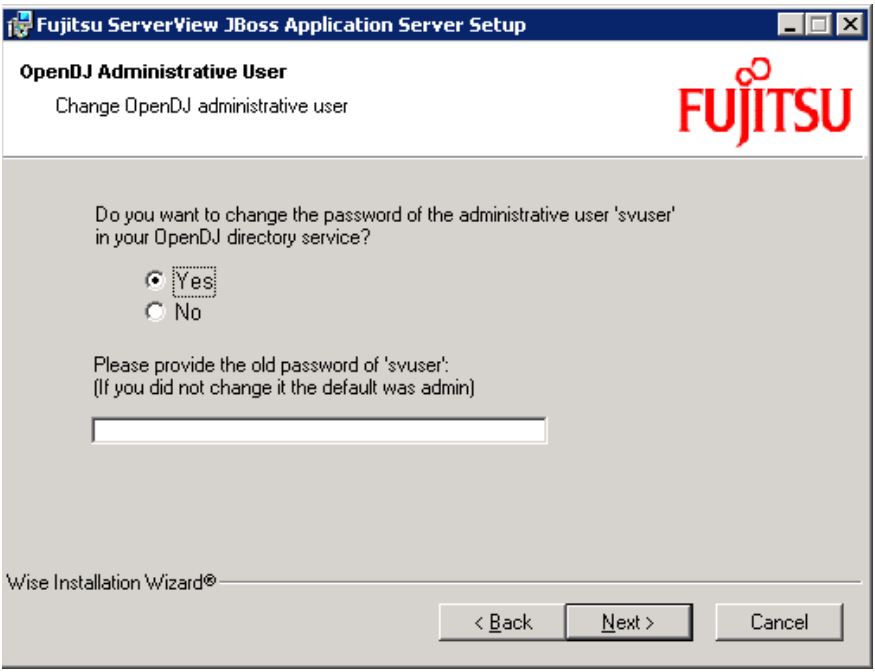

Fujitsu ServerView JBoss Application Server Setup
OpenDJ Administrative User
Change OpenDJ administrative user
FUJITSU
Do you want to change the password of the administrative user 'svuser' in your OpenDJ directory service?
Yes
No
Please provide the old password of 'svuser':
(If you did not change it the default was admin)
Wise Installation Wizard®
< Back
Next >
Cancel

Bild 6: Passwort von svuser konfigurieren (Windows)

Um das Passwort von *svuser* zu ändern, gehen Sie wie folgt vor:

1. Wählen Sie *Yes* und geben Sie das alte Passwort ein.
2. Klicken Sie auf *Next*, um fortzufahren.

   Der in Bild 5 auf Seite 41 abgebildete Dialog zur Definition eines neuen Passworts für *svuser* wird angezeigt.

Passwort von svuser auf Linux Systemen definieren / ändern

Erstmals definieren Sie das Passwort von *svuser* während der Installation des Operations Managers.

Ändern können Sie das Passwort jederzeit durch Ausführen des Kommandos *ChangeComputerDetails.sh*.

Zu Einzelheiten der Installation des Operations Managers siehe Handbuch "Installation ServerView Operations Manager Software unter Linux" .

3.2.2.3 Vordefinierte Passwörter der vordefinierten Benutzer Administrator, Monitor, Operator und UserManager ändern.

Beachten Sie:

Das vordefinierte Passwort der vordefinierten Benutzer *Administrator*, *Monitor*, *Operator* und *UserManager* lautet "admin". Aus Sicherheitsgründen wird dringend empfohlen, die vordefinierten Passwörter baldmöglichst zu ändern.

Die vordefinierten Passwörter *Administrator*, *Monitor*, *Operator* und *UserManager* können Sie über den Link *User Management* im Startfenster des Operation Managers ändern. Wenn ein Benutzer mit *UserAdministrator*-Rolle (oder einer darauf basierenden Rolle) den Link *User Management* anklickt, startet automatisch der *User Management*-Wizard. Mit dem *User Management*-Wizard können Sie alle vordefinierten Passwörter in einem einzigen Schritt ändern.

Nach erfolgreicher Installation des Operations Managers auf der zentralen Management-Station, besitzt zunächst nur der Benutzer *UserManager* die Berechtigungen der *UserAdministrator*-Rolle. Am günstigsten ist es deshalb, wenn der Benutzer *UserManager* alle vordefinierten Passwörter in einem einzigen Arbeistsschritt ändert.

Einzelheiten hierzu finden Sie unter Abschnitt "Benutzer, Rollen und Berechtigungen in OpenDJ verwalten" auf Seite 46.

3.2.3 LDAP-Portnummern von OpenDJ ändern

ServerView's OpenDJ ist konfiguriert für das Lauschen an Port 1473 (für unverschlüsselte LDAP-Verbindungen) sowie an Port 1474 (für SSL-verschlüsselte LDAP-Verbindungen). Normalerweise sollte es nicht erforderlich sein, diese Portnummern zu ändern. Lauscht jedoch eine weitere Anwendung auf Ihrer Management-Station (CMS) ebenfalls an einem der beiden Ports, so müssen Sie entweder die Konfiguration dieser Anwendung oder die Port-Konfiguration von OpenDJ ändern.

In der folgenden Erläuterung steht die Zeichenkette "dm_pw" als Platzhalter für das Passwort des OpenDJ Directory Managers. Die Zeichenfolgen "new_ldap_port" und "new_ldaps_port" sind Platzhalter für die neuen Portnummern des LDAP- bzw. LDAPS-Ports.

3.2.3.1 LDAP-Portnummern auf Windows Systemen ändern

Auf Windows Systemen ändern Sie die Portnummer wie folgt:

1. Öffnen Sie eine Windows Eingabeaufforderung.
2. Stellen Sie sicher, dass die Umgebungsvariablen `JAVA_HOME` und `OPENDS_JAVA_HOME` auf das Installationsverzeichnis der Java Laufzeitumgebung (Java Runtime Environment, JRE) gesetzt sind. Falls das JRE z.B. unter *C:\Program Files (x86)\Java\jre6* installiert ist, setzen Sie die Umgebungsvariablen mit den folgenden Kommandos:

   ```
   SET JAVA_HOME=C:\Programme (x86)\Java\jre7

   SET OPENDS_JAVA_HOME=C:\Programme (x86)\Java\jre7

   SET PATH=C:\Program Files (x86)\Java\jre7\bin
   ```

3. Wechseln Sie in das Verzeichnis *<ServerView directory>\opends\bat*.
4. Ändern Sie den LDAP-Port, indem Sie das folgende Kommando innerhalb einer einzelnen Zeile eingeben:

   ```
   dsconfig -D "cn=directory manager" -w dm_pw -n
   set-connection-handler-prop --handler-name "LDAP Connection
   Handler" --set listen-port:new_ldap_port
   ```

5. Ändern Sie den LDAP-Port, indem Sie das folgende Kommando innerhalb einer einzelnen Zeile eingeben:

   ```
   dsconfig -D "cn=directory manager" -w dm_pw -n
   set-connection-handler-prop --handler-name "LDAPS Connection
   Handler" --set listen-port:new_ldap_port
   ```

6. Starten Sie den Service ServerView JBoss Application Server 7 neu, um Ihre Einstellungen für den LADP- / LDAPS-Port zu aktivieren.

3.2.3.2 LDAP-Portnummern auf Linux Systemen ändern

Auf Linux-Systemen ändern Sie die Portnummer wie folgt:

1. Öffnen Sie eine Kommando-Shell.
2. Stellen Sie sicher, dass die Umgebungsvariablen `JAVA_HOME` und `OPENDS_JAVA_HOME` auf das Installationsverzeichnis der Java Laufzeitumgebung (Java Runtime Environment, JRE) gesetzt sind. Falls das JRE z.B. unter *usr/java/default* installiert ist, setzen Sie die Umgebungsvariablen mit den folgenden Kommandos:

   ```
   export JAVA_HOME=/usr/java/default
   ```

   ```
   export OPENDS_JAVA_HOME=/usr/java/default
   ```

3. Wechseln Sie in das Verzeichnis */opt/fujitsu/ServerViewSuite/opends/bin*.
4. Ändern Sie den LDAP-Port, indem Sie das folgende Kommando innerhalb einer einzigen Zeile eingeben:

   ```
   dsconfig -D "cn=directory manager" -w dm_pw -n
   set-connection-handler-prop --handler-name "LDAP Connection
   Handler" --set listen-port:new_ldap_port
   ```

5. Ändern Sie den LDAP-Port, indem Sie das folgende Kommando innerhalb einer einzigen Zeile eingeben:

   ```
   ./dsconfig -D "cn=directory manager" -w dm_pw -n
   set-connection-handler-prop --handler-name "LDAPS Connection
   Handler" --set listen-port:new_ldap_port
   ```

6. Starten Sie den Service ServerView JBoss Application Server 7 neu, um Ihre Einstellungen für den LADP- / LDAPS- Port zu aktivieren.

   ```
   /etc/init.d/sv_jboss restart
   ```

3.2.4 Benutzer, Rollen und Berechtigungen in OpenDJ verwalten

Der ServerView *UserManagement*-Wizard gestattet Ihnen die komfortable Benutzerverwaltung in ServerView mit OpenDJ. Im Einzelnen ermöglicht Ihnen der *User Management*-Wizard, die folgenden Aufgaben durchzuführen:

– Rollen erzeugen, ändern und löschen.

– Den Rollen Berechtigungen zuweisen.

– Rollen erzeugen, ändern und löschen.

– Den Benutzern Rollen zuweisen.

Um den *User Management*-Wizard zu nutzen, müssen Sie über die *UserAdministrator*-Rolle oder eine darauf basierende Rolle verfügen. Andernfalls können Sie lediglich Ihr eigenes Passwort ändern.

3.2.4.1 ServerView User Management starten.

Das ServerView User Management starten Sie im Startfenster der Operations Managers per Klick auf den Link *User Management*, den Sie unter *Security*. finden.

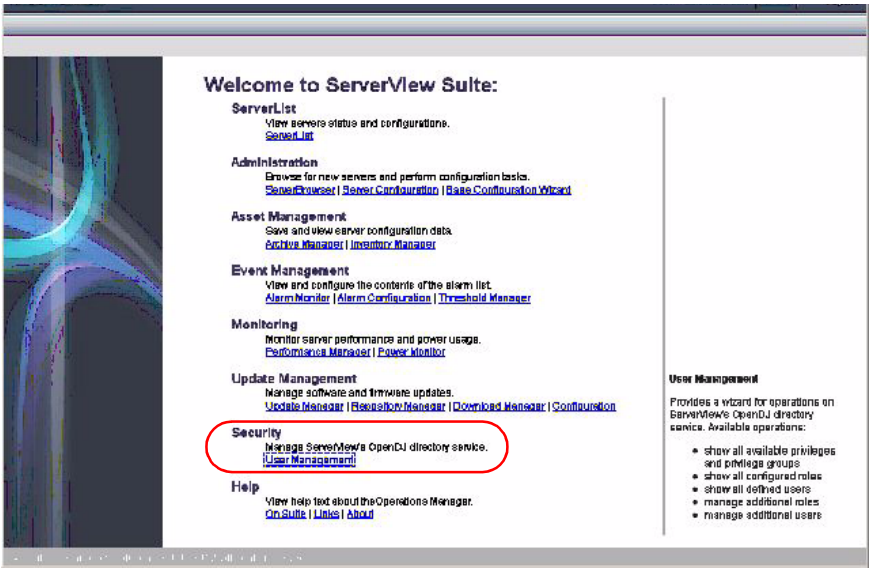

Welcome to ServerView Suite:
ServerList
View servers status and configurations.
ServerList
Administration
Browse for new servers and perform configuration tasks.
ServerBrowser | Server Configuration | Base Configuration Wizard
Asset Management
Save and view server configuration data.
Archive Manager | Inventory Manager
Event Management
View and configure the contents of the alarm list.
Alarm Monitor | Alarm Configuration | Threshold Manager
Monitoring
Monitor server performance and power usage.
Performance Manager | Power Monitor
Update Management
Manage software and firmware updates.
Update Manager | Repository Manager | Download Manager | Configuration
Security
Manage ServerView's OpenDJ directory service.
User Management
Help
View help text about the Operations Manager.
On Suite | Links | About
User Management
Provides a wizard for operations on ServerView's OpenDJ directory service. Available operations:
show all available privileges and privilege groups
show all configured roles
show all defined users
manage additional roles
manage additional users

Bild 7: ServerView Operations Manager - Startfenster

Der Link *User Management* wird nicht angezeigt, falls während der Installation des Operations Managers anstelle von OpenDJ ein anderer Verzeichnisdienst (z.B. Active Directory) ausgewählt wurde.

Je nachdem, ob Sie über die Berechtigung der Rolle *UserAdministrator* verfügen, gilt folgendes:

– Falls Sie nicht über die erforderlichen Berechtigungen verfügen, wird der Dialog zur Änderung Ihres eigenen Passworts angezeigt (siehe Seite 48).

– Falls Sie über die erforderlichen Berechtigungen verfügen, wird der *User Management*-Wizard gestartet (siehe Seite 49).

3.2.4.2 Eigenes OpenDJ-Passwort ändern

Mit diesem Dialog können Sie Ihr eigenes OpenDJ-Passwort ändern.

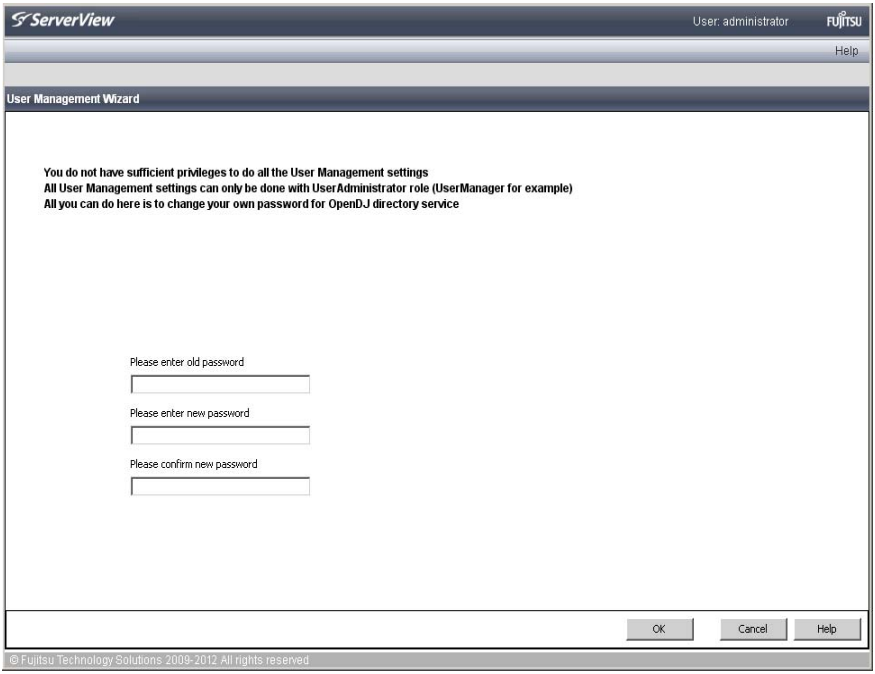

ServerView
User: administrator
FUJITSU
Help
User Management Wizard
You do not have sufficient privileges to do all the User Management settings
All User Management settings can only be done with UserAdministrator role (UserManager for example)
All you can do here is to change your own password for OpenDJ directory service
Please enter old password
Please enter new password
Please confirm new password
OK
Cancel
Help
© Fujitsu Technology Solutions 2009-2012. All rights reserved.

Bild 8: Dialog zur Änderung des eigenen OpenDJ-Passworts

Please insert old password
: Geben Sie Ihr altes Passwort ein.

Please insert new password
: Geben Sie Ihr neues Passwort ein.

Please confirm the new password
: Wiederholen Sie zur Bestätigung die Eingabe des neuen Passworts.

OK
: Aktiviert das neue Passwort.

Cancel
: Schließt den Dialog, ohne das Passwort zu ändern.

3.2.4.3 User Management-Wizard

Nach dem Start zeigt der *User Management*-Wizard zunächst den Dialog *Role Definitions* an:

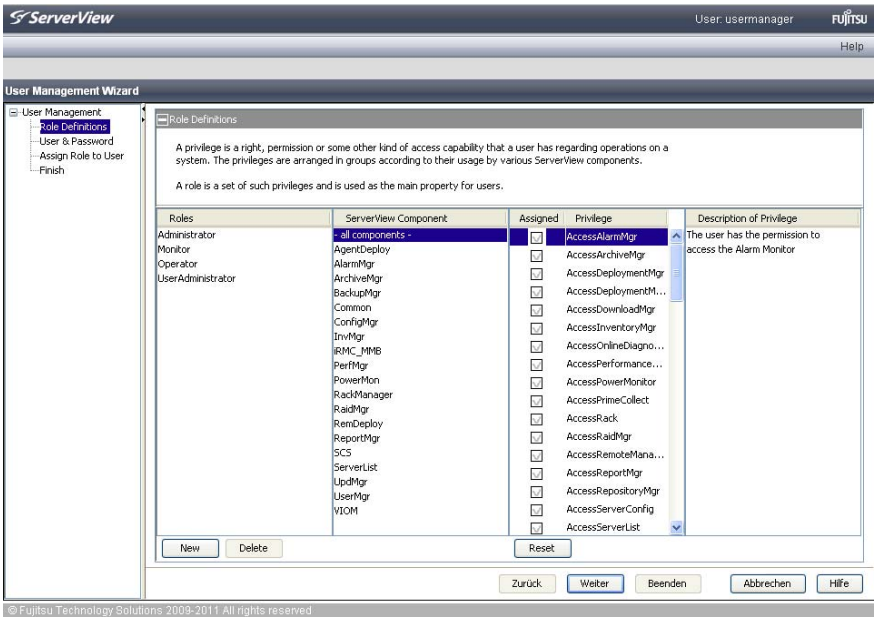


Bild 9: User Management-Wizard - Dialog "Role Definitions"

Der *User Management*-Wizard umfasst vier Schritte. Die Reihenfolge der Schritte wird in der Baumstruktur auf der linken Seite angezeigt. Sie müssen diese Schritte jedoch nicht unbedingt in dieser Reihenfolge bearbeiten. Vielmehr können Sie jeden der drei Schritte *Role Definition*, *User&Password* und *Assign Role to User* unabhängig von den anderen Schritten durchführen. Nach Eingabe Ihrer Einstellungen können Sie mit im Schritt *Finish* Ihre Einstellungen aktivieren und den Wizard verlassen.

Mit Schaltflächen, die unten rechts in jedem Dialog angeordnet sind, können Sie den Wizard durchlaufen:

Zurück
: Öffnet den vorausgehenden Schritt des Wizards.

Weiter
: Öffnet den nächsten Schritt des Wizards.

Beenden

Schließt den Wizard und aktiviert alle Ihre Einstellungen.

Die Schaltfläche *Beenden* ist nur im Dialogschritt *Finish* aktiviert.

Abbrechen

Beendet den Wizard, ohne Ihre Einstellungen zu aktivieren.

Im Folgenden finden Sie eine detaillierte Beschreibung zu den Dialogen des *User Management*-Wizards.

Role Definitions

Im Dialog *Role Definitions* können Sie neue Rollen definieren, existierende Rollen löschen sowie Berechtigung-zu-Rolle-Zuordnungen aktivieren/deaktivieren. Der Dialog zeigt tabellarisch alle zurzeit definierten Rollen mit den zugehörigen Privilegien an.

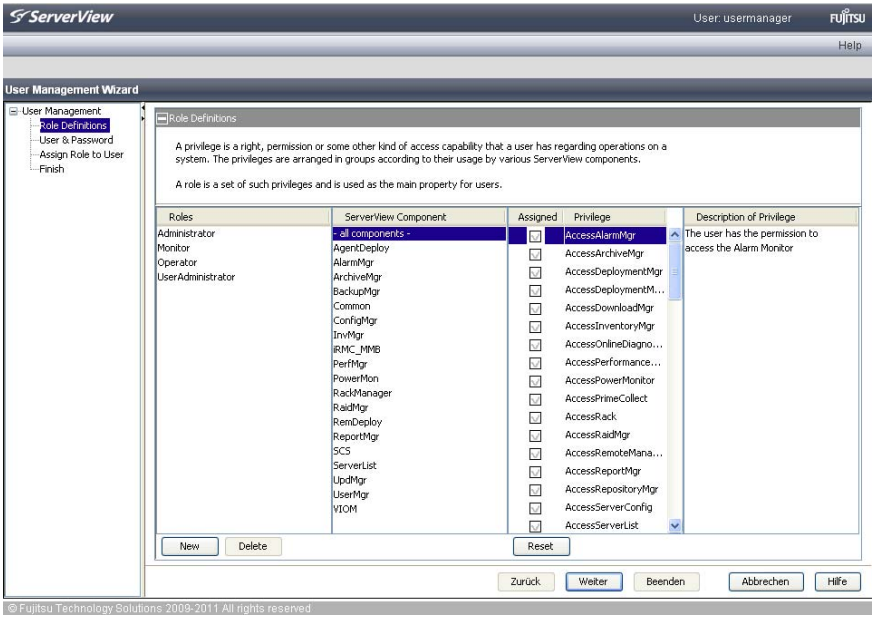


Bild 10: User Management-Wizard - Dialog "Role Definitions"

Roles

Listet alle zurzeit definierten Rollen auf. Die vordefinierten Rollen *Administrator*, *Monitor*, *Operator* und *UserAdministrator* werden oben in der Liste angezeigt. Wenn Sie eine Rolle auswählen, werden die zugehörigen Berechtigungen in der Spalte *Privilege* angezeigt.

ServerView Component

Listet alle vorhandenen Privilegien-Kategorien (Privilege Categories) auf, wobei jede Privilegien-Kategorie alle Berechtigungen zusammenfasst, die für die Benutzung einer bestimmten ServerView-Komponente oder zur Ausführung einer bestimmten Aufgabe erforderlich sind. Durch Auswahl einer oder mehrerer Kategorieren können Sie die unter *Assigned Privilege* angezeigten Berechtigungen auf diejenigen Berechtigungen reduzieren, die zu den ausgewählten Kategorien gehören.

Für weitere Informationen siehe Abschnitt "Privilegien-Kategorien und zugehörige Berechtigungen" auf Seite 118.

Assigned Privilege

Listet alle vorhandenen Berechtigungen auf. Wenn Sie unter *ServerView Component* eine oder mehrere Kategorien ausgewählt haben, sind nur die zu den ausgewählten Kategorien gehörigen Berechtigungen sichtbar. Sie können eine Berechtigung-zu-Rolle-Zuordnung aktivieren/deaktivieren, indem Sie die zugeordnete *Assigned*-Option auswählen/abwählen.

Die Zuordnung von Berechtigungen zu den vordefinierten Rollen *Administrator*, *Monitor*, *Operator* und *UserAdministrator* kann nicht verändert werden. Die entsprechenden Optionen für die Berechtigung-zu-Rolle-Zuordnung sind unveränderbar ("ausgegraut").

Description of Privilege

Liefert Kurzbeschreibung zur ausgewählten Berechtigung.

New

Per Klick auf *New* öffnen Sie den Dialog *New Role*:

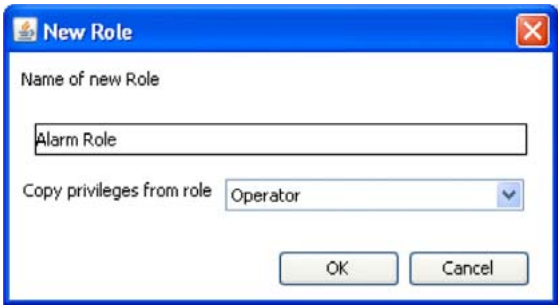


Bild 11: User Management-Wizard - Neue Rolle definieren

Name of newrole

Name der neuen Rolle

Copy privileges from role

Hier können Sie eine früher definierte Rolle aus einer Liste auswählen. Die der ausgewählten Rolle zugeordneten Berechtigungen werden dann automatisch der neuen Rolle zugeordnet.

OK

Aktiviert die neue Rolle und schließt den Dialog *New Role*. Die neue Rolle wird nun unter *Roles* angezeigt.

Cancel

Beendet den Dialog *New Role* ohne eine neue Rolle zu definieren.

Delete

Löscht die ausgewählte Rolle.

Reset

Setzt die aktuell angezeigten Berechtigung-zu-Rolle-Zuordnungen auf die zuletzt abgespeicherten Einstellungen zurück.

User & Password

Der Dialog *User & Password* listet alle zurzeit in OpenDJ definierten Benutzer/Passwort-Kombinationen auf und ermöglicht die Ausführung der folgenden Operationen:

– Neue Benutzer definieren.

– Passwörter vorhandener Benutzer ändern.

– Vorhandene Benutzer löschen.

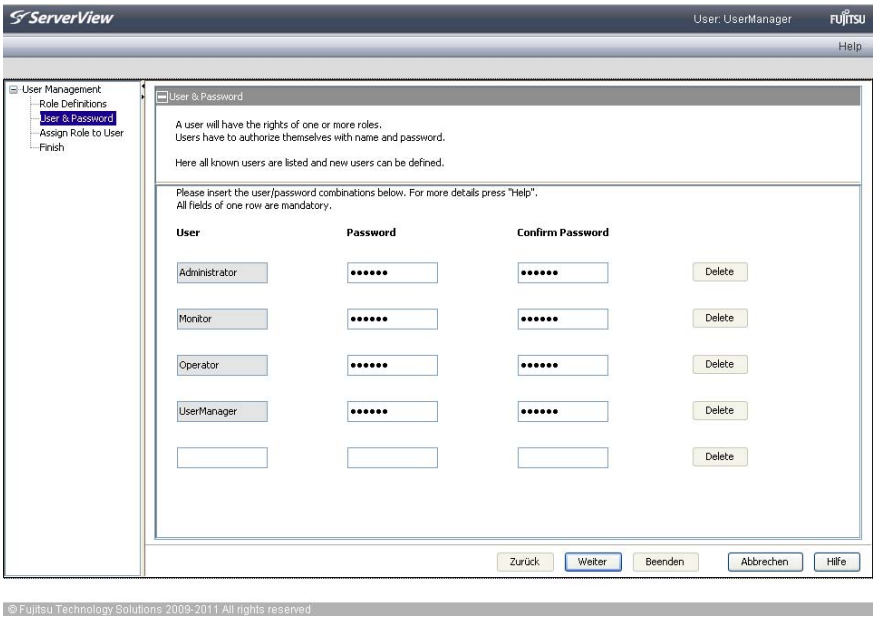


Bild 12: User Management-Wizard - Dialog "User & Password"

Die vier vordefinierten Benutzer *Administrator*, *Monitor*, *Operator* und *UserManager* sind oben in der Liste angeordnet und können nicht gelöscht werden. Die Passwörter von *Administrator*, *Monitor*, *Operator* und *UserManager* können Sie jedoch ändern.

Mindestens eine freie Zeile mit leeren Eingabefeldern für *User*, *Password* und *Confirm Password* wird unten in der Liste angezeigt und ermöglicht Ihnen das Definieren neuer Benutzer.

User

Benutzername

Passwort

Neues Passwort

Confirm Password

Wiederholen Sie zur Bestätigung die Eingabe des neuen Passworts.

Delete

Löscht den zugehörigen Benutzer.

Reset

Setzt die Einstellungen für den zugehörigen Benutzer auf die zuletzt abgespeicherten Einstellungen zurück.

Assign Role to User

Der Dialog *Assign Role to User* gestattet Ihnen, Rollen-zu-Benutzer-Zuordnungen zu definieren und aufzulösen. Der Dialog zeigt alle definierten Benutzer und Rollen tabellarisch an. Markiert sind alle Rollen, die dem aktuell ausgewählten Benutzer zugeordnet sind.

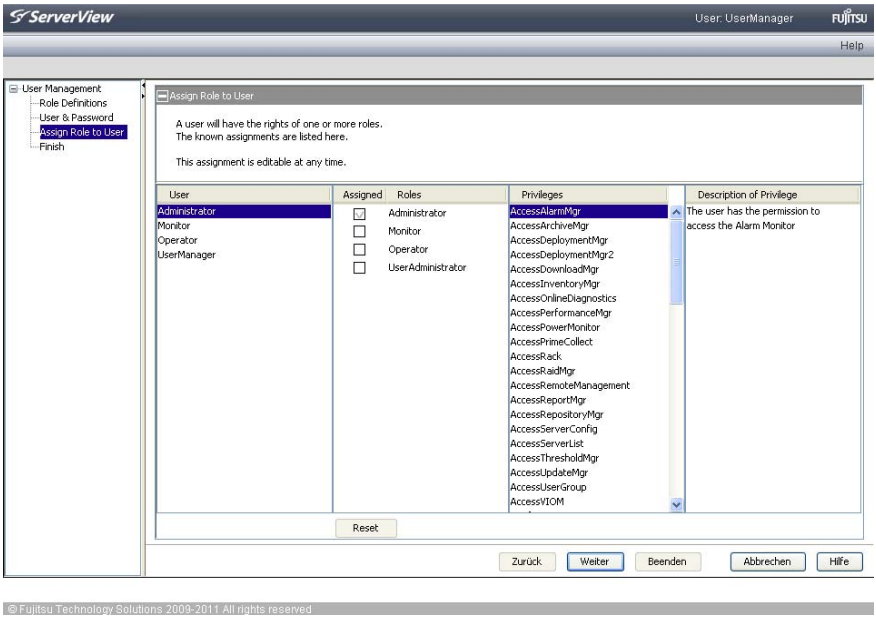


Bild 13: User Management-Wirzard: Dialog "Assign Role to User"

User

Listet alle definierten Benutzer auf. Wenn Sie einen Benutzer auswählen, werden die dem Benutzer zurzeit zugeordneten Rollen in der Spalte *Assigned Roles* mit markierter *Assigned*-Option angezeigt.

Die vier vordefinierten Benutzer *Administrator*, *Monitor, Operator* und *UserManager* sind oben in der Liste angeordnet und können nicht gelöscht werden. Die Zuordnung von Rollen zu diesen Benutzern kann nicht verändert werden.

Assigned Roles

Listet alle definierten Rollen auf. Jeder Rolle ist eine *Assigned*-Option vorangestellt, die anzeigt, ob die zugehörige Rolle derzeit dem ausgewählten Benutzer zugeordnet ist (Option ausgewählt) oder nicht (Option abgewählt).

Sie können eine Berechtigung-zu-Rolle-Zuordnung aktivieren/deaktivieren, indem Sie die zugeordnete *Assigned*-Option auswählen/abwählen.

Privileges

Zeigt die Gesamtheit der Berechtigungen an, die den Rollen des ausgewählten Benutzers zugeordnet sind.

Description of Privilege

Kurzbeschreibung zur ausgewählten Berechtigung.

Reset

Setzt die Benutzer-zu-Rolle-Zuordnungen auf die zuletzt abgespeicherten Einstellungen zurück.

Finish

Der Dialog *Finish* zeigt eine Zusammenfassung der von Ihnen in der aktuellen *User Management*-Sitzung durchgeführten Schritte an. Per Klick auf *Beenden* aktivieren Sie Ihre Einstellungen und schließen den Wizard.

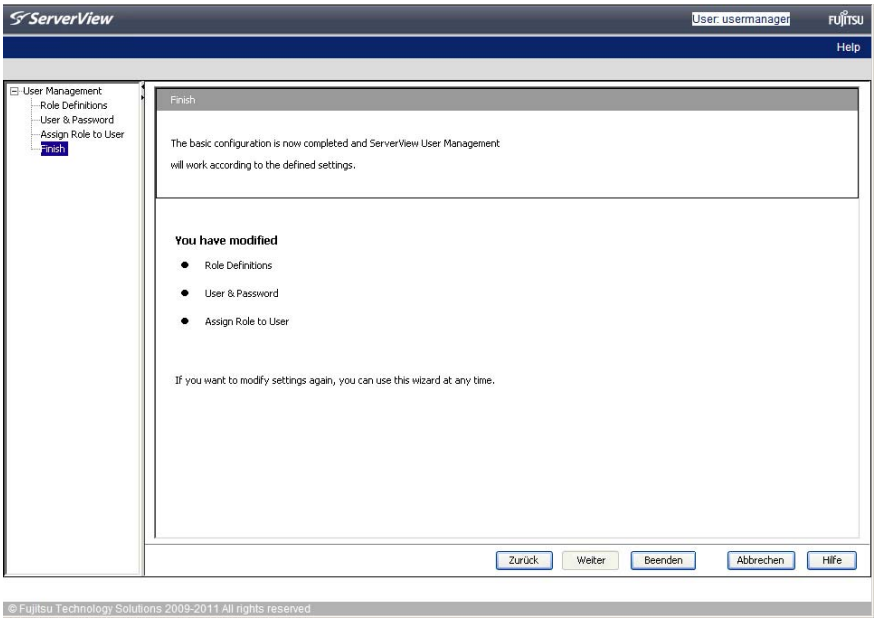


Bild 14: User Management-Wizard - Dialog "Finish"

3.2.5 iRMC S2/S3/S4 in die ServerView-Benutzerverwaltung mit OpenDJ und SSO integrieren

Die Konfiguration des iRMC S2/S3/S4 für die Integration in die ServerView-Benutzerverwaltung mit OpenDJ sowie für die Teilnahme an der ServerView Suite SSO-Domäne umfasst zwei Schritte, die Sie über die iRMC S2/S3/S4-Web-Oberfläche durchführen können:

1. Den iRMC S2/S3/S4 für den zusammen mit dem Operations Manager installierten Verzeichnisdienst OpenDJ konfigurieren.
2. Die iRMC S2/S3/S4-Web-Oberfläche für die CAS-basierte Single Sign-on (SSO)-Authentifizierung innerhalb der ServerView Suite konfigurieren.

Wichtiger Hinweis:

Der CAS Service muss für alle iRMC S2/S3/S4 konfiguriert werden, die an der SSO-Domäne teilnehmen (siehe Handbücher "iRMC S2/S3 - integrated Remote Management Controller" und "iRMC S4 - integrated Remote Management Controller").

Die folgende Beschreibung legt den Schwerpunkt auf die Einstellungen die erforderlich sind für die Integration eines iRMC S2/S3/S4 in die ServerView-Benutzerverwaltung mit OpenDJ und für die Teilnahme an der ServerView Suite SSO-Domäne. Allgemeine Informationen zur Verzeichnisdienst- und CAS-Konfiguration des iRMC S2/S3/S4 finden Sie in den Handbüchern "iRMC S2/S3 - integrated Remote Management Controller" und "iRMC S4 - integrated Remote Management Controller".

3.2.5.1 iRMC S2/S3/S4 in die ServerView-Benutzerverwaltung mit OpenDJ und SSO integrieren

Auf der Seite *Verzeichnisdienst Konfiguration* der iRMC S2/S3/S4-Web-Oberfläche können Sie den iRMC S2/S3/S4 für die globale Benutzerverwaltung mit dem Verzeichnisdienst OpenDJ konfigurieren, der zusammen mit dem Operations Manager installiert wurde. Die erforderlichen Einstellungen sind in Bild 15 dargestellt und werden anschließend erläutert.

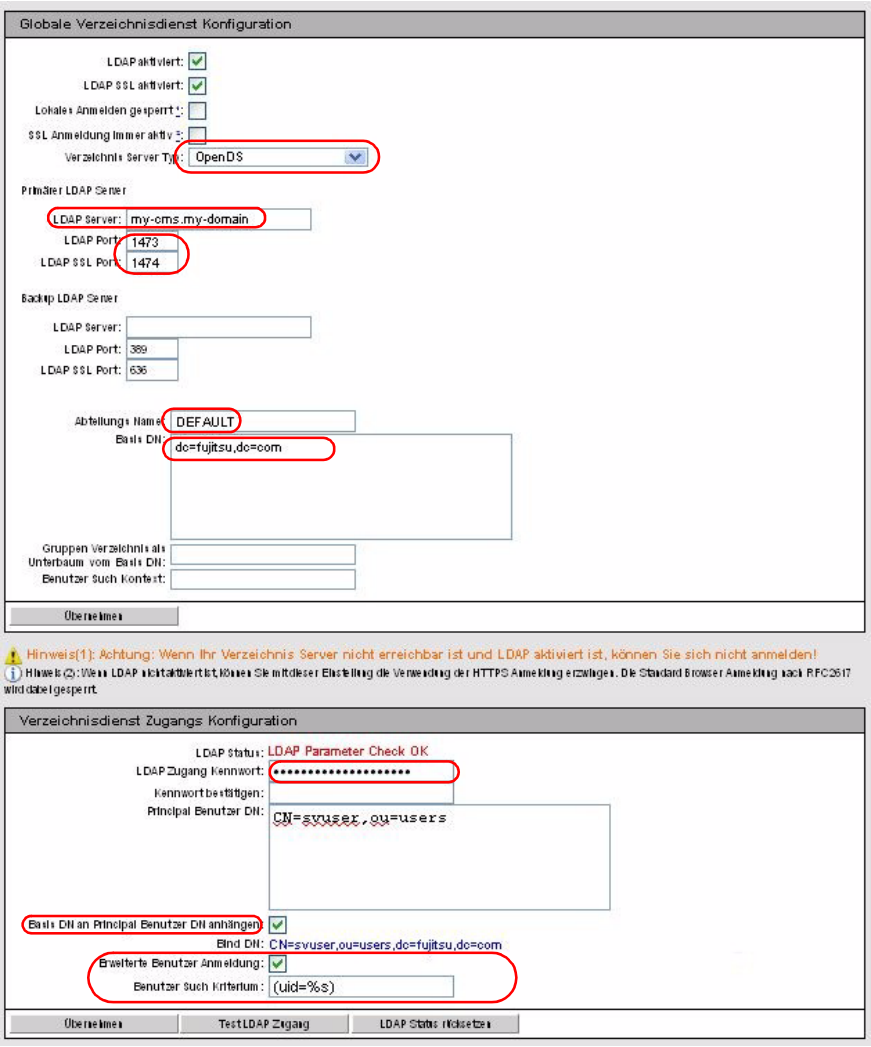


Bild 15: iRMC S2/S3/S4 für die Benutzerverwaltung mit OpenDS / OpenDJ konfigurieren

Erforderliche Einstellungen in der Gruppe "Globale Verzeichnisdienst Konfiguration":

1. Wählen Sie *LDAP aktiviert* und *LDAP SSL aktiviert*.
2. Wählen Sie *OpenDS* unter *Verzeichnis Server Typ* und klicken Sie auf *Übernehmen*.
3. Konfigurieren Sie unter *Primärer LDAP Server* die folgenden Einstellungen:
   - *LDAP Server*: DNS-Name der zentralen Management-Station.

     Sie sollten hier den selben Namen angeben, den Sie bei der Installation des Operations Managers auf der Management-Station angegeben haben.
   - *LDAP Port*: 1473
   - *LDAP SSL Port*: 1474
4. Spezifizieren Sie unter *Abteilungs Name* das Defaul-Department `DEFAULT`.
5. Spezifizieren Sie unter *Basis DN*: `dc=fujitsu,dc=com`
6. Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu aktivieren.

Erforderliche Einstellungen in der Gruppe "Verzeichnisdienst Zugangs Konfiguration":

1. Geben Sie unter *Principal Benutzer DN* ein: `cn=svuser,ou=users`
2. Wählen Sie *Basis DN an Principal Benutzer DN anhängen.*
3. Wählen Sie *Erweiterte Benutzer Anmeldung* und klicken Sie auf *Übernehmen*.
4. Geben Sie unter *Benutzer Such Kriterium* ein: `(uid=%s)`
5. Klicken Sie auf *Test LDAP Zugang*, um den Status Ihrer LDAP-Verbindung zu testen, der anschließend unter *LDAP Status* angezeigt wird.
6. Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu aktivieren.

3.2.5.2 iRMC S2/S3/S4-Web-Oberfläche für CAS-basierte Single Sign-on (SSO)-Authentifizierung konfigurieren.

Auf der Seite *Centralized Authentication Service (CAS) Konfiguration* iRMC S2/S3/S4-Web-Oberfläche können Sie die Web-Oberfläche des zugehörigen iRMC S2/S3/S4 für die CAS-basierte Single Sign-on (SSO)-Authentifizierung konfigurieren.

Bild 15 zeigt die erforderlichen Einstellungen:

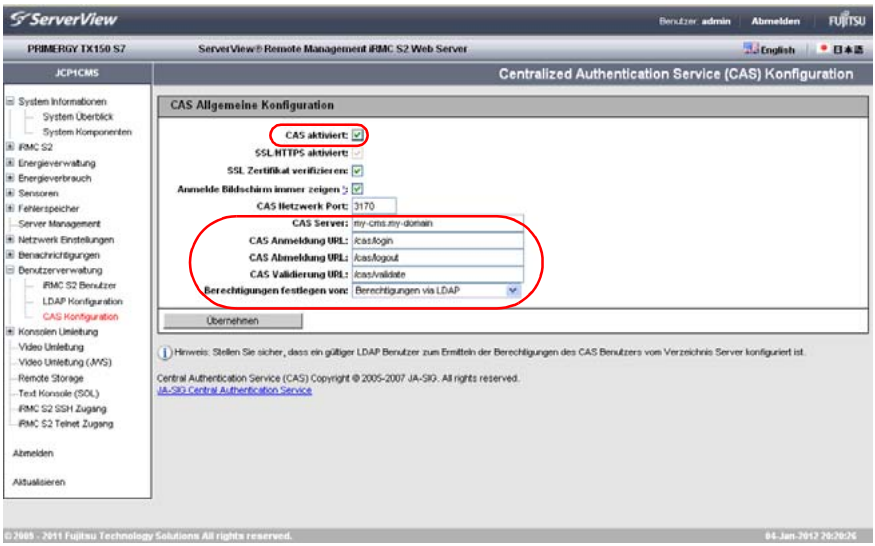


Bild 16: iRMC S2/S3/S4 für die Teilnahme an der ServerView Suite-SSO-Domäne konfigurieren

Konfigurieren Sie die folgenden Einstellungen:

1. Wählen Sie *CAS aktiviert*.
2. Geben Sie unter *CAS Server* den DNS-Namen der zentralen Management-Station ein.

   Alle Systeme, die zur SSO-Domäne gehören, müssen die zentrale Management-Station (CMS) unbedingt über dieselbe Adressstruktur referenzieren. (Eine SSO-Domäne umfasst alle Systeme, deren Authentifizierung über denselben CAS-Service erfolgt.) Wenn Sie also z. B. den ServerView Operations Manager unter der Bezeichnung „my-cms.my-domain“ installiert haben, müssen Sie zur Konfiguration des CAS-Services für ein iRMC S2/S3/S4 genau dieselbe Bezeichnung angeben. Geben Sie dagegen nur „my-cms“ oder eine andere IP-Adresse von my-cms an, wird die SSO-Funktionalität zwischen den beiden Systemen nicht aktiviert.

3. Lassen Sie die unter die unter *CAS Anmeldung URL* und *CAS Abmeldung URL* und *CAS Validierung URL* die voreingestellten Werte (*/cas/login*, */cas/logout*, */cas/validate*) unverändert.
4. Wählen Sie die Option *SSL Zertifikate verifizieren*.

   Aus Sicherheitsgründen wird dringend empfohlen, die Verifizierung von SSL-Zertifikaten zu aktivieren. Zusätzlich zur Auswahl der Option *SSL Zertifiate verifizieren* erfordert die Verifizierung von SSL Zertifikaten, dass das Server-Zertifikat der Management-Station in den Truststore des iRMC S2/S3/S4 geladen ist. Einzelheiten zum Hochladen eines SSL-Zertifikats auf den iRMC S2/S3/S4 finden Sie in den Handbüchern "iRMC S2/S3 - integrated Remote Management Controller" und "iRMC S4 - integrated Remote Management Controller".

5. Wählen Sie unter *Berechtigungen festlegen von* die Option *Berechtigungen via LDAP*.
6. Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu aktivieren.

3.2.6 OpenDJ-Daten sichern und wiederherstellen

Dieser Abschnitt beschreibt, wie Sie die OpenDJ-Kommandos *backup* und *restore* auf der zentralen Management-Station verwenden, um die folgenden Aufgaben auszuführen:

– Backup der internen Datenbank des OpenDJ-Verzeichnisservers erstellen

– Interne Datenbank des OpenDJ-Verzeichnisservers aus einem anwendbaren Backup wiederherstellen

ACHTUNG!

Bei der Wiederherstellung der internen Datenbank des OpenDJ-Verzeichnisservers **muss** ein Backup verwendet werden, das mit derselben Operations Manager-Version erstellt wurde, die aktuell auf der Management-Station ausgeführt wird.

Wenn auf eine neuere Operations Manager-Version gewechselt wird, muss immer ein neues Backup erstellt werden. Wichtige Informationen, die mit Operations Manager bereitgestellt wurden, können andernfalls bei der Wiederherstellung verloren gehen.

Wenn Sie seit der Erstellung des zu verwendenden Backups Passwörter geändert haben, werden diese Änderungen bei der Wiederherstellung überschrieben.

3.2.6.1 OpenDJ-Daten auf Windows-Systemen sichern und wiederherstellen

Um die interne Datenbank des OpenDJ-Verzeichnisservers zu **sichern**, gehen Sie wie folgt vor:

1. Stoppen Sie den Dienst *ServerView JBoss Application Server 7*.
2. Öffnen Sie die Eingabeaufforderung im Ordner *....\ServerView Suite\opends\bat*.
3. Geben Sie folgenden Befehl ein:

   ```
   backup.bat –n userRoot –d <path to the backup directory>
   ```

4. Starten Sie den Dienst *ServerView JBoss Application Server 7*.

Um die interne Datenbank des OpenDJ-Verzeichnisservers **wiederherzustellen**, gehen Sie wie folgt vor:

1. Stoppen Sie den Dienst *ServerView JBoss Application Server 7*.
2. Öffnen Sie die Eingabeaufforderung im Ordner ....*ServerView Suite\opends\bat*.
3. Geben Sie folgenden Befehl ein: <`restore.bat –d <path to the backup directory>`
4. Starten Sie den Dienst *ServerView JBoss Application Server 7*.

3.2.6.2 OpenDJ-Daten auf Linux-Systemen sichern und wiederherstellen

Um die interne Datenbank des OpenDJ-Verzeichnisservers zu **sichern**, gehen Sie wie folgt vor:

1. Stoppen Sie den JBoss-Dienst: `/etc/init.d/sv_jboss stop`
2. `cd /opt/fujitsu/ServerViewSuite/opends/bin`
3. `su svuser`
4. Geben Sie folgenden Befehl ein: `sh backup –n userRoot –d <path to the backup directory>`
5. `exit`
6. Starten Sie den JBoss-Dienst: `/etc/init.d/sv_jboss start`

Um die interne Datenbank des OpenDJ-Verzeichnisservers **wiederherzustellen**, gehen Sie wie folgt vor:

1. Stoppen Sie den JBoss-Dienst: `/etc/init.d/sv_jboss stop`
2. `cd /opt/fujitsu/ServerViewSuite/opends/bin`
3. `su svuser`
4. Geben Sie folgenden Befehl ein: `sh restore –d <path to the backup directory>`
5. `exit`
6. Starten Sie den JBoss-Dienst: `/etc/init.d/sv_jboss start`

3.3 ServerView-Benutzerverwaltung in Microsoft Active Directory integrieren

Beachten Sie:

Die Konfiguration der Einstellungen für die Benutzerverwaltung von ServerView und iRMC S2/S3/S4 erfordert detaillierte Active Directory-Kenntnisse. Nur Personen, die über hinreichende Kenntnisse verfügen, sollten die Konfiguration durchführen.

Um die Benutzerverwaltung in ServerView mit Active Directory abwickeln zu können, müssen Sie die folgenden vorbereitenden Schritte durchführen:

1. Rollendefinitionen der ServerView Suite (*Administrator*, *Operator*, *Monitor*, siehe Seite 36) in Active Directory importieren.
2. Rollendefinitionen für den iRMC S2/S3/S4 in Active Directory importieren.
3. Rollen den Benutzern zuordnen.
4. Sicheren LDAP-Zugang (LDAPS) auf den Active Directory Server konfigurieren.

Diese Schritte sind nachfolgend detailliert beschrieben.

Voraussetzungen:

Die folgenden Dateien werden benötigt für die Interaktion von ServerView- und iRMC S2/S3/S4-Benutzerverwaltung in Active Directory:

- **Für die Benutzerverwaltung in ServerView:**

  Sie benötigen eine Datei im LDIF (Lightweight Directory Interchange Format)-Format, die die ServerView-spezifischen Strukturen für die Integration in Active Directory enthält.

  Falls Sie während Installation des Operations Managers Active Directory als zu verwendenden Verzeichnisdienst gewählt haben, finden Sie die benötigte LDIF-Datei im folgenden Verzeichnis der zentralen Management-Station, auf der der Operations Manager installiert ist:

  – Auf Windows Systemen:
  <ServerView directory>\svcommon\files\SVActiveDirectory.ldif

  – Auf Linux Systemen:
  /opt/fujitsu/ServerViewSuite/svcommon/files/SVActiveDirectory.ldif

- **Für die iRMC S2/S3/S4-Benutzerverwaltung:**

  XML-Konfigurationsdatei, die die Strukturinformationen in XML-Syntax für die Struktur *SVS* in Active Directory enthält. Der *SVS_LdapDeployer* (siehe Seite 162) erzeugt LDAP-Strukturen auf Basis dieser *XML*-Konfigurationsdatei. Die Syntax der Konfigurationsdatei ist dargestellt in den Beispiel-Konfigurationsdateien *Generic_Settings.xml* und *Generic_InitialDeploy.xml*, die zusammen mit dem *jar*-Archiv *SVS_LdapDeployer.jar* auf der ServerView Suite DVD ausgeliefert werden.

Wichtiger Hinweis:

Die Abwicklung sowohl der ServerView- als auch des iRMC S2/S3/S4-Benutzerverwaltung innerhalb derselben Organizational Unit (OU) *SVS* setzen voraus, dass der iRMC S2/S3/S4 als Element des Departments *DEFAULT* konfiguriert ist.

Gehen Sie wie folgt vor:

1. **Importieren Sie die in ServerView definierten Benutzerrollen.**

   a) Kopieren Sie die Datei *SVActiveDirectory.ldif* in ein temporäres Verzeichnis auf dem Windows System, auf dem Active Directory läuft.

   b) Öffnen Sie die Windows Eingabeaufforderung, und wechseln Sie in das Verzeichnis, das die Datei *SVActiveDirectory.ldif* enthält.

   c) Importieren Sie die LDIF-Datei mithilfe des Microsoft-Tools *ldifde*:

   ```
   ldifde -i -e -k -f SVActiveDirectory.ldif
   ```

   Falls das *ldifde*-Tool nicht in der Umgebungsvariablen (*PATH variable*) Ihres Systems eingetragen ist, finden Sie es im Verzeichnis *%WINDIR%\system32*.

   Falls erforderlich, wird eine bereits vorhandene LDAP-Struktur um neue Berechtigungen erweitert. Bereits existierende Einträge sind jedoch nicht betroffen.

   Die hinzugefügten Berechtigungen (Privilegien) und Rollen werden nun in der Benutzeroberfläche von Active Directory angezeigt (siehe Bild 17 auf Seite 67).

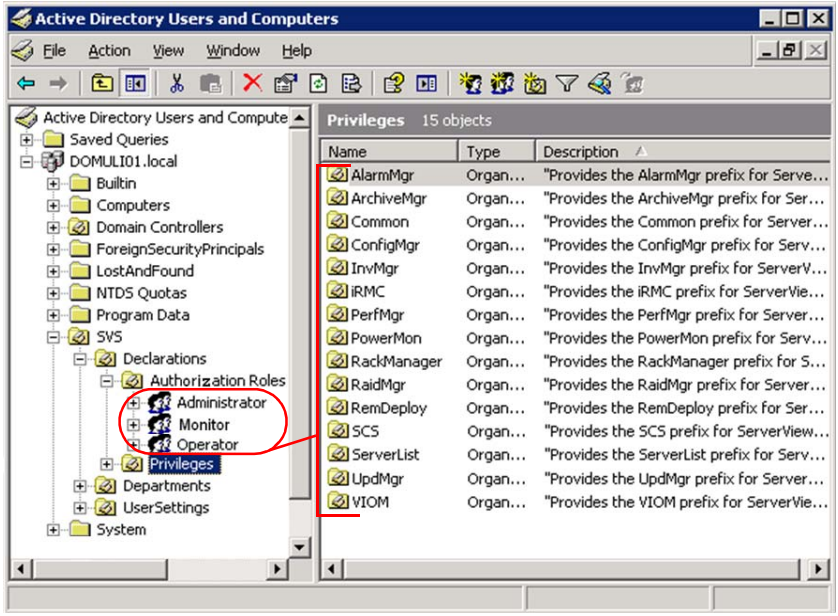

Active Directory Users and Computers
File Action View Window Help
Active Directory Users and Compute
Saved Queries
DOMULI01.local
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
LostAndFound
NTDS Quotas
Program Data
SVS
Declarations
Authorization Roles
Administrator
Monitor
Operator
Privileges
Departments
UserSettings
System
Privileges 15 objects
Name Type Description
AlarmMgr Organ... "Provides the AlarmMgr prefix for Serve...
ArchiveMgr Organ... "Provides the ArchiveMgr prefix for Ser...
Common Organ... "Provides the Common prefix for Server...
ConfigMgr Organ... "Provides the ConfigMgr prefix for Serv...
InvMgr Organ... "Provides the InvMgr prefix for ServerV...
iRMC Organ... "Provides the iRMC prefix for ServerVie...
PerfMgr Organ... "Provides the PerfMgr prefix for Server...
PowerMon Organ... "Provides the PowerMon prefix for Serv...
RackManager Organ... "Provides the RackManager prefix for S...
RaidMgr Organ... "Provides the RaidMgr prefix for Server...
RemDeploy Organ... "Provides the RemDeploy prefix for Ser...
SCS Organ... "Provides the SCS prefix for ServerView...
ServerList Organ... "Provides the ServerList prefix for Serv...
UpdMgr Organ... "Provides the UpdMgr prefix for Server...
VIOM Organ... "Provides the VIOM prefix for ServerVie...

Bild 17: Die hinzugefügten Privilegien und Rollen werden im Active Directory GUI angezeigt.

2. **Importieren Sie die iRMC S2/S3/S4-Benutzerrollen.**

   Verwenden Sie für den Import der iRMC S2/S3/S4-Rollendefinitionen in Active Directory das Tool *SVS_LdapDeployer*. Einzelheiten hierzu finden Sie unter Abschnitt "SVS_LdapDeployer - Strukturen „SVS“ und „iRMCgroups“ generieren, pflegen und löschen" auf Seite 162.

3. **Ordnen Sie den Benutzern und Gruppen Benutzerrollen zu.**

   In den nachfolgend beschriebenen Schritten wird exemplarisch angenommen, dass Sie die dem Benutzer „John Baker“ (Login-Name „NYBak“ in Ihrer Active Directory Domäne „DOMULI01“) die *Monitor*-Rolle zuweisen wollen.

   Die nachfolgend beschriebenen Schritt gelten auch für die Zuweisung von Rollen an iRMC S2/S3/S4-Benutzer. Näheres zur Zuweisung von Rollen an iRMC S2/S3/S4-Benutzer finden Sie in Abschnitt "iRMC S2/S3-Benutzer einer Rolle (Berechtigungsgruppe) zuordnen" auf Seite 176 und Abschnitt "iRMC S4-Benutzer einer Rolle (Berechtigungsgruppe) zuordnen" auf Seite 256.

   Bitte stellen Sie sicher, dass die LDAP-Objekte mit den Anmeldeinformationen für den Benutzer, dem Sie Rollen zuordnen wollen, unter der konfigurierten User Search Base liegen. (Die User Search Base wird beim Einrichten des ServerView Operations Managers konfiguriert - siehe entsprechendes Installationshandbuch.)

   Ebenso, wenn Sie einer Gruppe eine Rolle zuordnen wollen: Bitte stellen Sie sicher, dass die LDAP-Objekte mit den Anmeldeinformationen aller Mitglieder unter der konfigurierten User Search Base liegen.

   a) Wählen Sie an der Management-Station *Start - Systemsteuerung - Administrative Tools - Active Directory Benutzer und Computer*, um die grafische Benutzeroberfläche von Active Directory zu starten.

   b) Durchlaufen Sie in Baumstruktur den Knoten *SVS* von oben nach unten bis zum Knoten *Departments*. Expandieren Sie die Departments *CMS* und *DEFAULT* (siehe Bild 18):

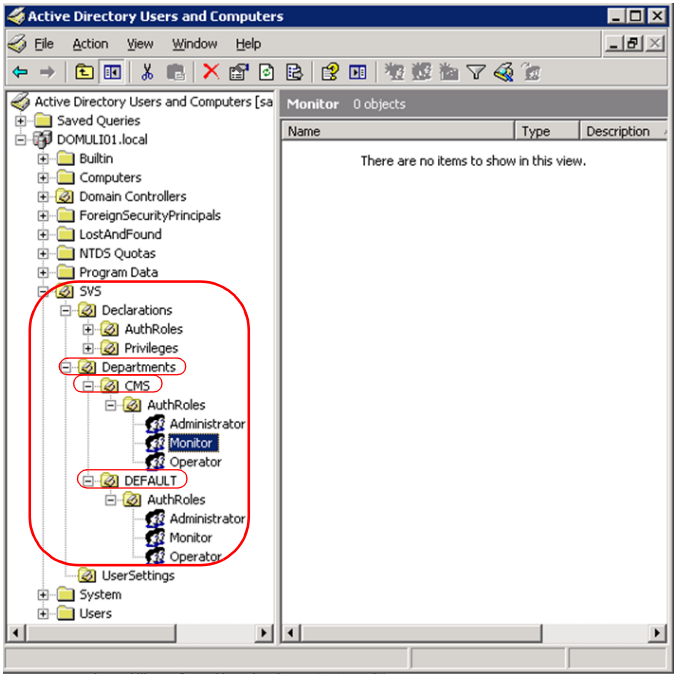


Bild 18: Die Monitor-Rolle soll einem Benutzer (John Baker) zugewiesen werden.

c) Wählen Sie *SVS - Departments - CMS - AuthRoles*, klicken Sie mit der rechten Maustaste auf *Monitor* und wählen Sie *Properties*.

Der Dialog *Properties* für die Monitor-Rolle wird angezeigt:

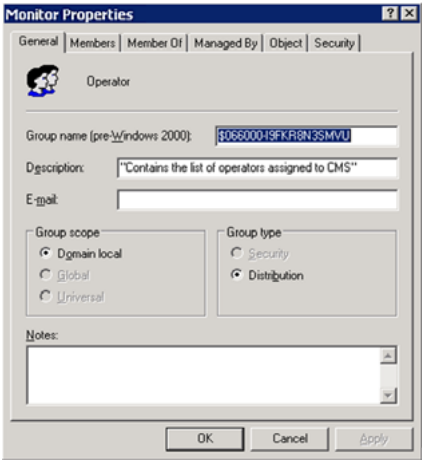


Bild 19: Dialog Monitor Properties für die Monitor-Rolle

d) Wählen Sie die Registerkarte *Members* und klicken Sie auf *Add...* .

Bild 20: Dialog Properties für die Monitor-Rolle - Registerkarte Members

Der Dialog *Select Users...* wird angezeigt.

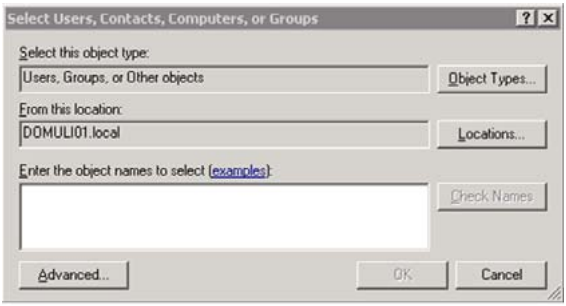


Bild 21: Dialog Select Users...

e) Klicken Sie auf *Advanced...* .

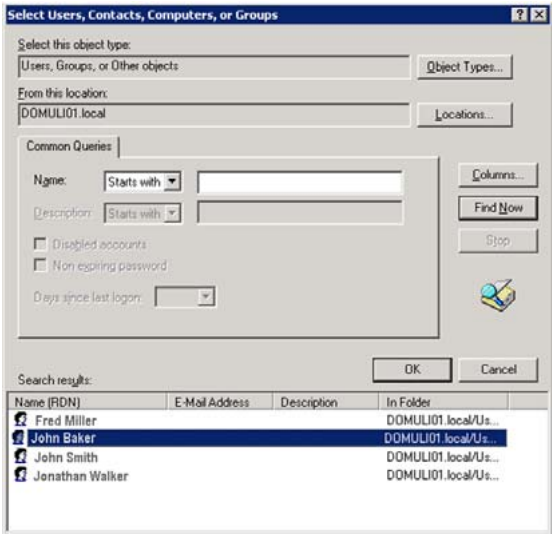


Bild 22: Gewünschten Benutzer auswählen

Es kann hilfreich sein, die Spalte *Name (RDN)* (Login-Name) in der Liste *Search results* auszuwählen und durch Eingrenzen von *Name* die Suche per Klick auf *Find Now* zu beschleunigen.

f) Wählen Sie den gewünschten Benutzer oder oder die Gruppe und klicken Sie auf *OK*.

Der Benutzer „Baker“ wird nun in der Liste *object names* des übergeordneten Dialogs angezeigt:

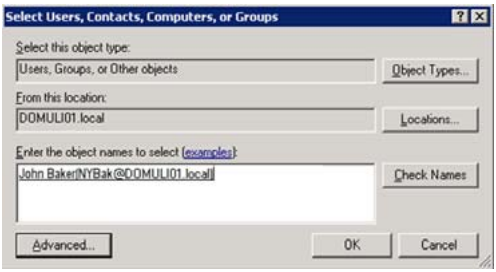


Bild 23: Select Users... Dialog: Benutzer "Baker" wird angezeigt.

g) Klicken Sie auf *OK*.

Der Benutzer „Baker“ wird nun in der Registerkarte *Members* des Dialogs *Monitor Properties* angezeigt:

Bild 24: Dialog Properties für Monitor - Registerkarte Members: Benutzer „Baker“ wird angezeigt.

h) Wiederholen Sie die Schritte *c* bis *g* für das Department *DEFAULT*.

4. Konfigurieren Sie den sicheren LDAP-Zugang (LDAPS) zum Active Directory Server.

   Die Installation des Operations Managers erfordert die Konfiguration des LDAP-Zugriffs auf den Verzeichnisserver, auf den die Benutzerverwaltung durchgeführt wird. Standardmäßig stellt Active Directory eine ungesicherte LDAP-Schnittstelle auf Port 389 zur Verfügung. Diese Schnittstelle können Sie zu Testzwecken nutzen.

   Wenn Sie jedoch eine Produktivumgebung aufsetzen wollen, sollten Sie auf Ihrem Active Directory Server eine sichere LDAPS-Schnittstelle einrichten. Hierfür müssen Sie auf diesem Server ein Server-Zertifikat zu installieren.

   Detaillierte Informationen hierzu finden Sie in der entsprechenden Microsoft-Dokumentation *"How to enable LDAP over SSL with a third-party certification authority"* unter *http://support.microsoft.com*.

   Detaillierte Informationen zur Konfiguration des LDAP/SSL-Zugriffs auf den iRMC S2/S3/S4 finden Sie im Abschnitt "LDAP/SSL-Zugriff des iRMC S2/S3 am Active Directory Server konfigurieren" auf Seite 171 oder in Abschnitt "LDAP/SSL-Zugriff des iRMC S4 am Active Directory Server konfigurieren" auf Seite 251.

   Zu Testzwecken genügt es, auf dem Active Directory Server ein selbstsigniertes Zertifikat zu installieren. Mit dem Microsoft-Tool *selfssl.exe* aus den IIS 6.0 Resource Kit Tools (herunterladbar unter *http://support.microsoft.com*) können Sie dies sehr einfach durchführen.

   Beispiel:

   Um ein selbstsignierten Zertifikats mit einer 2048 bit Schlüssellänge und einer Gültigkeitsdauer von zwei Jahren auf dem Server *myserver.mydomain* zu installieren, gehen Sie wie folgt vor:

   ► Öffnen Sie eine Windows Eingabeaufforderung und geben Sie das folgende Kommando ein:

   ```
   selfssl /T /N:CN=myserver.mydomain /K:2048 /V:730
   ```

   selfssl.exe gibt die folgenden Meldungen aus:

   ```
   Microsoft (R) SelfSSL Version 1.0

   Copyright (C) 2003 Microsoft Corporation. All rights
   reserved.

   Do you want to replace the SSL settings for site 1
   (Y/N)?
   ```

► Geben Sie "Y" ein.

Die anschließend angezeigte Meldung "Failed to build the subject name blob: 0x80092023" können Sie ignorieren, da die Meldung nur darauf hinweist, dass IIS nicht installiert ist.

Wenn künftig via *ldaps: //myserver.mydomain* auf Active Directory zugegriffen wird, wird Active Directory das soeben das installierte Zertifikat verwenden.

Der Benutzer „John Baker“ kann sich nun am Operations Manager unter dem Benutzernamen „NYBak“ anmelden. Baker kann nun alle Funktionen ausführen, die mit den Berechtigungen (Privilegien) der Benutzerrolle *Monitor* zulässig sind.

3.3.1 Passwort des LDAP-Bind-Kontos ändern

Sie können das Passwort des LDAP-Bind-Kontos, das für den Zugriff auf "externe" Verzeichnisdienste wie Active Directory verwendet wird, auf die gleiche Weise ändern, wie in Abschnitt "Passwort von svuser definieren / ändern." auf Seite 41 beschrieben.

Alternativ können Sie das Batch-Skript *SetDSPassword* verwenden. Dieses Skript hat den Vorteil, dass kein Neustart von JBoss durchgeführt wird. Beachten Sie jedoch, dass es bis zu fünf Minuten dauern kann, bis die Konfigurationsänderungen übernommen werden. Sie sollten daher nach Änderung des Passworts immer fünf Minuten warten, bevor Sie versuchen, sich erneut anzumelden.

SetDSPassword kann in einer Windows- oder Linux-Umgebung aufgerufen werden:

Windows

- Öffnen Sie die Windows Eingabeaufforderung.
- Wechseln Sie in das Verzeichnis *<ServerView directory>\jboss\standalone\bin*.
- Geben Sie *SetDSPassword <neues Passwort>* ein.

  – Das Passwort darf alle druckbaren Zeichen, darunter Leerzeichen ( ) und doppelte gerade Anführungszeichen ("), enthalten.

  – Wenn das Passwort Leerzeichen ( ), doppelte gerade Anführungszeichen ("), Kommas (,), Zirkumflexe (^) oder andere Sonderzeichen enthält, muss es von doppelten Anführungszeichen eingeschlossen werden, z. B. "Pa\\w^rd".

  – Umgekehrte Schrägstriche (\) werden buchstabengetreu interpretiert, es sei denn sie stehen direkt vor einem doppelten geraden Anführungszeichen.

  – Ein doppeltes gerades Anführungszeichen, vor dem ein umgekehrter Schrägstrich (\) steht, wird buchstabengetreu als doppeltes gerades Anführungszeichen (") interpretiert.

  – Ein Zirkumflex (^) wird nicht als Maskierungszeichen oder Begrenzungszeichen interpretiert, wenn das Passwort von doppelten geraden Anführungszeichen umgeben ist.

Linux

- ► Öffnen Sie ein Terminal, wie z.B. Xterm oder Gnome-term.
- ► Wechseln Sie in das Verzeichnis */opt/fujitsu/ServerViewSuite/jboss/standalone/bin*.
- ► Geben Sie *./SetDSPassword <neues Passwort>* ein.

  – Das Passwort darf alle druckbaren Zeichen, darunter Leerzeichen ( ) und doppelte gerade Anführungszeichen ("), enthalten.

  – Wenn das Passwort Leerzeichen ( ), doppelte gerade Anführungszeichen ("), Kommas (,), ein Zirkumflex (^) oder andere Sonderzeichen enthält, muss es von doppelten Anführungszeichen eingeschlossen werden, z. B. "Pa\\w^rd".

  – Umgekehrte Schrägstriche (\) werden buchstabengetreu interpretiert, es sei denn sie stehen direkt vor einem doppelten geraden Anführungszeichen.

  – Ein doppeltes gerades Anführungszeichen, vor dem ein umgekehrter Schrägstrich (\) steht, wird buchstabengetreu als doppeltes gerades Anführungszeichen (") interpretiert.

  – Ein Zirkumflex (^) wird nicht als Maskierungszeichen oder Begrenzungszeichen interpretiert, wenn das Passwort von doppelten geraden Anführungszeichen umgeben ist.

3.3.2 LDAP Password Policy Enforcement (LPPE)

Wenn ein Benutzer versucht, sich bei CAS zu authentifizieren, können verschiedene Sonderfälle (Ausnahmen) eintreten:

– Login derzeit nicht möglich

– Passwort ist abgelaufen/muss zurückgesetzt werden

– Benutzerkonto deaktiviert/abgelaufen/gesperrt

Ohne LPPE würde der normale CAS-Login-Vorgang die oben stehenden Szenarios als Fehler interpretieren, was eine Authentifizierung verhindern würde. LPPE verbessert das standardmäßige CAS-Login, indem die folgenden Schritte ausgeführt werden:

1. LPPE unterbricht den standardmäßigen Authentifizierungsvorgang, indem Fehlercodes erfasst werden, die als Teil der Nutzlast der LDAP-Antwort zurückgegeben werden.
2. LPPE übersetzt die Fehlercodes in sehr viel präzisere Fehlerangaben und gibt diese Fehlerangaben im Rahmen des CAS-Login-Vorgangs aus.

Auf diese Weise kann der Benutzer geeignete Maßnahmen ergreifen.

Die derzeit von LPPE verarbeiteten Anmeldeausnahmen werden in Tabelle 3 aufgeführt.

LDAP-Fehlercode	LDAP-Fehlertext	Von CAS angezeigte Meldung
530	Login derzeit nicht zulässig	Bei der Authentifizierung wird eine Meldung angezeigt, dass der Benutzer sich derzeit nicht anmelden kann: *You are not permitted to logon at this time. Please try again later.*
531	Login an dieser Workstation nicht zulässig	Bei der Authentifizierung wird eine Meldung angezeigt, dass das Konto deaktiviert wurde und dass der Benutzer sich an einen Administrator wenden soll: *You are not permitted to logon at this workstation. Please try again later.*
532	Passwort abgelaufen	Bei der Authentifizierung wird eine Meldung angezeigt, dass das Kontopasswort abgelaufen ist. Optional wird ein Link zu einer Self-Service-Anwendung zur Passwortverwaltung bereitgestellt: *Your password has expired. Please change your password.*

Tabelle 3: LDAP-Fehlercodes

LDAP-Fehlercode	LDAP-Fehlertext	Von CAS angezeigte Meldung
533	Konto deaktiviert	Bei der Authentifizierung wird eine Meldung angezeigt, dass das Konto deaktiviert wurde und dass der Benutzer sich an einen Administrator wenden soll: *This account has been disabled.* *Please contact the system administrator to regain access.*
701	Konto abgelaufen	Bei der Authentifizierung wird eine Meldung angezeigt, dass das Konto abgelaufen ist: *Your account has expired.*
773	Benutzer muss das Passwort zurücksetzen	Bei der Authentifizierung wird eine Meldung angezeigt, dass das Kontopasswort geändert werden muss. Optional wird ein Link zu einer Self-Service-Anwendung zur Passwortverwaltung bereitgestellt: *You must change your password.* *Please change your password.*
775	Benutzerkonto gesperrt	Bei der Authentifizierung wird eine Meldung angezeigt, dass das Konto deaktiviert wurde und dass der Benutzer sich an einen Administrator wenden soll: *This account has been disabled.* *Please contact the system administrator to regain access.*

Tabelle 3: LDAP-Fehlercodes

Passwortablauf

LPPE erkennt zudem den erwarteten Ablauf eines Benutzerpassworts. Wenn das Passwort demnächst abläuft, wird dies innerhalb eines konfigurierten Warnzeitraums angezeigt. Bei der Authentifizierung zeigt CAS eine Meldung an, dass das Benutzerpasswort demnächst abläuft:

Your password expires today!
Please change your password now.

oder

Your password expires tomorrow!
Please change your password now.

oder

Your password expires in … days.
Please change your password now.

Um das erwartete Ablaufdatum zu ermitteln, liest das CAS einige LDAP-Attribute aus dem konfigurierten Active Directory-Service. Zu diesem Zweck sind die folgenden Konfigurationswerte erforderlich:

Domain DN

Dabei handelt es sich um den *Distinguished Name* der Active Directory-Domäne.

Beispiel

```
dc=fujitsu,dc=com
```

Valid Days

Der Wert dieser Eigenschaft bestimmt die Anzahl Tage, die ein Passwort gültig ist. Beachten Sie, dass hiermit der Standardwert für den Fall definiert wird, dass kein Attribut *maxPwdAge* in Active Directory gefunden wird. Das bedeutet, dass ein in Active Directory konfigurierter Wert immer die Einstellung hier überschreibt.

Beispiel

```
90
```

Warning Days

Der Wert dieser Eigenschaft bestimmt die Anzahl Tage, die ein Benutzer vor Ablauf des Passworts gewarnt wird. Beachten Sie, dass es in Active Directory kein entsprechendes Attribut gibt. Das bedeutet, dass dieser Wert hier die einzige Definition für die Warnzeit des Passwortablaufs ist.

Beispiel

```
30
```

Password URL (optional)

Dieser Eintrag bestimmt die URL, an die der Benutzer umgeleitet wird, um das Passwort zu ändern. Die Landing Page dieser URL muss vom Benutzer bereitgestellt werden - Serverview bietet keine entprechende Web-Seite an. Wenn es keine entsprechende Seite in der Umgebung des Benutzers gibt, sollte die Konfigurationsoption weggelassen werden.

Dieser Eintrag ist optional, normalerweise werden Passwörter über die Verwaltung des Active Directory-Verzeichnisdienstes geändert.

Beispiel

```
https://www.example.corp.com/UserMgt
```

4 SSL-Zertifikate für Authentifizierung verwalten

Für die Kommunikation mit Web-Browsern und verwalteten Servern („Managed Nodes“) verwendet die Management-Station eine Public Key-Infrastruktur (PKI) mit sicheren SSL-Verbindungen.

Dieses Kapitel liefert Informationen zu folgenden Themen:

– "SSL-Zertifikate verwalten (Überblick)" auf Seite 82
– "SSL-Zertifikate auf der Management-Station verwalten" auf Seite 85
– "Verwalteten Server Systeme für Role Based Access (RBAC) und Client-Authentifizierung einrichten" auf Seite 101

4.1 SSL-Zertifikate verwalten (Überblick)

Für die Kommunikation mit Web-Browsern und verwalteten Servern („Managed Nodes“) verwendet die Management-Station eine Public Key-Infrastruktur (PKI) mit sicheren SSL-Verbindungen.

Die Management-Station authentisiert sich beim Web-Browser via Server-Authentifizierung

Web-Browser kommunizieren mit der Management-Station immer über eine HTTPS-Verbindung, also über eine sichere SSL-Verbindung. Deshalb benötigt der JBoss Web-Server auf der Management-Station ein Zertifikat (X.509 Zertifikat), um sich gegenüber dem Web-Browser mittels Server-Authentifizierung zu authentisieren. Das X.509-Zertifikat enthält alle für die Identifizierung des JBoss Web-Servers benötigten Informationen sowie den öffentlichen Schlüssel (Public Key) des JBoss Web-Servers.

Einzelheiten hierzu finden Sie im Abschnitt "SSL-Zertifikate auf der Management-Station verwalten" auf Seite 85.

Die Management-Station authentisiert sich gegenüber dem verwalteten Server via Client-Authentifizierung

Ein verwalteter Server (z.B. PRIMERGY Server), auf dem die RBAC-Funktionalität genutzt wird, erfordert Client-Authentifizierung auf der Basis von X.509-Zertifikaten. Deshalb muss sich eine Management-Station beim Verbindungsaufbau zum verwalteten Server authentisieren. Client-Authentifizierung schützt den verwalteten Server sowohl vor dem Zugriff einer nicht vertrauenswürdigen Management-Station als auch vor dem Zugriff einer nicht-privilegierten Anwendung, die auf der Management-Station läuft.

Client-Authentifizierung setzt voraus, dass das Zertifikat einer vertrauenswürdigen Management-Station zuvor auf dem verwalteten Server installiert wurde.

Einzelheiten hierzu finden Sie im Abschnitt "Verwalteten Server Systeme für Role Based Access (RBAC) und Client-Authentifizierung einrichten" auf Seite 101.

SSL Public Key-Datei und Konfigurationsdatei des Security-Interceptors

Während der Installation des Operation Managers werden folgende Dateien automatisch erzeugt:

- *<system_name>.scs.pem*

  Selbst-signiertes Zertifikat im PEM-Format. Die PEM-Datei enthält außerdem den öffentlichen Schlüssel (Public Key).

  Eine zentrale Management-Station verwendet die Datei *<system_name>.scs.pem* für folgende Zwecke:

  – Server-Authentifizierung gegenüber Web-Browsern, die sich mit der Management-Station verbinden.

  – Client-Authentifizierung gegenüber den verwalteten Servern, auf denen die RBAC-Funktionalität genutzt wird. Für die Client-Authentifizierung muss die Datei *<system_name>.scs.pem* auf dem verwalteten Server installiert werden.

- *<system_name>.scs.xml*

  Konfigurationsdatei des Security-Interceptors. Diese Datei wird intern für Validierungsaufrufe verwendet. Für die Aktivierung der RBAC-Funktionalität auf dem verwalteten Server muss die Datei *<system_name>.scs.xml* auf dem verwalteten Server installiert werden.

Der Operations Manager Installations-Wizard installiert beide Dateien in folgendem Verzeichnis der Management-Station:

– *<ServerView directory>\svcommon\data\download\pki* (auf Windows Systemen)

– */opt/fujitsu/ServerViewSuite/svcommon/data/download/pki* (auf Linux Systemen)

Im Folgenden werden die Dateien *<system_name>.scs.pem* und *<system_name>.scs.xml* kurz Zertifikatsdateien genannt.

Schlüsselpaare verwalten - keystore- und truststore-Dateien

Das Java-basierte Schlüssel- und Zertifikatsmanagement auf dem JBoss Web-Server verwaltet Schlüsselpaare und Zertifikate mithilfe zweier Dateien.

– In der keystore-Datei (Dateiname: *keystore*) speichert der JBoss Web-Server seine eigenen Schlüsselpaare und Zertifikate.

– Die truststore-Datei (Dateiname: *cacerts*) enthält alle Zertifikate, die der JBoss Web-Server als vertrauenswürdig einstuft.

keystore- und truststore-Datei liegen im folgenden Verzeichnis:

– *<ServerView directory>\jboss\standalone\svconf\pki* (auf Windows-Systemen)

– */opt/fujitsu/ServerViewSuite/jboss/standalone/svconf/pki* (auf Linux-Systemen)

Für die Verarbeitung von keystore- und truststore-Datei verwenden Sie das *keytool* -Utility (siehe Seite 89).

4.2 SSL-Zertifikate auf der Management-Station verwalten

Web-Browser kommunizieren mit der Management-Station immer über eine HTTPS-Verbindung, also über eine sichere SSL-Verbindung. Deshalb benötigt der JBoss Web-Server auf der Management-Station ein Zertifikat (X.509 Zertifikat), mit dem er sich gegenüber dem Web-Browser via Server-Authentifizierung authentisiert. Das X.509-Zertifikat enthält alle für die Identifizierung des JBoss Web-Servers benötigten Informationen sowie den öffentlichen Schlüssel (Public Key) des JBoss Web-Servers.

4.2.1 Bei der Installation wird automatisch ein selbstsigniertes Zertifikat erzeugt

Während der Installation des Operation Managers wird für den lokalen JBoss Web-Server automatisch ein selbstsigniertes Zertifikat im PEM-Format (<*system_name*>.*scs.pem*) erzeugt.

Das Setup installiert die Datei <*system_name*>.*scs.pem* im folgenden Verzeichnis:

– <*ServerView directory*>*svcommon\data\download\pki* (auf Windows Systemen)

– */opt/fujitsu/ServerViewSuite/svcommon/data/download/pki* (auf Linux Systemen)

Bei der Verwendung eines selbstsignierten Zertifikats brauchen Sie sich nicht um die Einrichtung Ihrer eigenen Zertifizierungsstelle (Certificate Authority, CA) oder um die Versendung einer Zertifikatsanforderung (Certificate Signing Request, CSR) an eine externe Zertifizierungsstelle zu kümmern.

Wenn eine Update-Installation des ServerView Operations Managers benötigt wird (z.B. nachdem der Name der Management-Station geändert wurde), wird das selbstsignierte Zertifikat automatisch während der Update-Installation ersetzt.

Wenn der JBoss Web Server ein selbstsigniertes Zertifikat verwendet: Wenn sich die Web-Browser mit dem JBoss Web Server verbinden, werden sie einen Zertifikatsfehler melden mit Empfehlungen, was zu tun ist.

Aufgrund ihrer hohen Verfügbarkeit eignen sich selbstsignierte Zertifikate besonders für Testumgebungen. Um jedoch die hohen Sicherheitsstandards zu erfüllen, die typisch sind für das produktive Server-Management mit dem Operations Manager, empfehlen wir Ihnen die Verwendung eines so genannten Zertifizierungsstellenzertifikats, das von einer vertrauenswürdigen Zertifizierungsstelle signiert ist.

4.2.2 Zertifizierungsstellenzertifikat (CA Certificate) erzeugen

Zertifizierungsstellenzertifikate werden von einer zentralen Instanz, der Zertifizierungsstelle (Certificate Authority, CA), herausgegeben.Die Zertifizierungsstelle signiert die Zertifikate mit dem privaten Schlüssel der Zertifizierungsstelle, nachdem sie die Identität der im Zertifikat genannten Organisation geprüft hat. Die Signatur, die Bestandteil des Zertifikats ist, wird beim Verbindungsaufbau offengelegt, sodass der Client die Vertrauenswürdigkeit des Zertifikats verifizieren kann.

Beachten Sie:

Wenn eine Update-Intallation des ServerView Operations Managers erforderlich ist (z.B. nachdem der Name der Management-Station geändert wurde), wird das Zertifikat der Zertifizierungsstelle **nicht** automatisch während der Update-Installation ersetzt. Stattdessen müssen Sie das Zertifikat durch Ihr eigenes ersetzen (siehe Abschnitt "Zertifikat auf der zentralen Management-Station ersetzen" auf Seite 90).

Folgende Schritte sind zur Erzeugung eines Zertifizierungsstellenzertifikats erforderlich:

1. Erzeugen Sie eine Zertifikatsanforderung (Certificate Signing Request, CSR, hier: *certrq.pem*), z.B. mit dem Tool *openssl*:

   ```
   openssl req -new -keyout privkey.pem -out certreq.pem
   -days 365
   ```

2. Senden Sie die Zertifikatsanforderung an die Zertifizierungsstelle.

   Die Zertifizierungsstelle gibt das signierte Zertifikat (Certificate Reply) zurück, z.B. im PEM-Format als *certreply.pem* oder im DER-Format als *certreply.cer*.

   Im Folgenden wird angenommen, dass das Zertifikat das PEM-Format hat. Wenn nötig, können Sie das Zertifikat vom DER-Format in das PEM-Format mit folgendem Kommando konvertieren:

   ```
   openssl x509 -in certreply.cer -inform DER -out
   certreply.pem -outform PEM
   ```

Wenn das Zertifikat erweiterte Key-Usages enthalten soll, ist es wichtig, dass es für die Key-Usages Server-Authentifizierung (1.3.6.1.5.5.7.3.1) und Client-Authentfizierung (1.3.6.1.5.5.7.3.2) signiert wird, weil es sowohl als Server-Zertifikat als auch als Client-Zertifikat verwendet wird.

3. Speichern Sie das signierte Zertifikat in einer Datei ab.
4. Verifizieren Sie das signierte Zertifikat.

4.2.3 Software-Tools zur Zertifikats- und Schlüsselverwaltung

Für die Verwaltung von Zertifikaten und zugehörigen Schlüsseln werden folgende Tools benötigt:

– *openssl*

  Das *openssl* -Tool können Sie aus dem Internet herunterladen, z.B. von der Shining Light Productions Website (*http://www.slproweb.com*). Alternativ empfiehlt sich auch die Installation der Cygwin-Umgebung (*http://www.cygwin.com*).

  Wenn Sie das Tool *openssl* von der Shining Light Productions-Website verwenden, müssen Sie die Umgebungsvariable *OPENSSL_CONF* auf folgenden Wert setzen:

  < path to the OpenSSL installation directory>/bin/openssl.cfg

– *keytool*

  Das *keytool* können Sie von der Oracle Homepage herunterladen. Da das *keytool* neben der Java Virtual Machine installiert wird, ist das Utility standardmäßig auf der Management-Station vorhanden:

  – Auf Windows Systemen: z.B. unter *C:\Program Files (x86)\Java\jre7\bin*

  – Auf Linux Systemen: */usr/java/default/bin*

4.2.4 Zertifikat auf der zentralen Management-Station ersetzen

Dieser Abschnitt beschreibt, welche Schritte erforderlich sind, um ein Zertifikat durch ein anderes zu ersetzen.

Voraussetzungen:

Die nachfolgend beschriebenen Schritte setzen voraus:

– Erforderliche Software: *openssl*, *keytool* (siehe Seite 89).

  Zusätzlich wird in der nachfolgenden Erläuterung angenommen, dass das Verzeichnis, in dem das *keytool* liegt, Bestandteil der Pfad-Variablen (*PATH* variable) ist.

– Es müssen vorhanden sein: ein signiertes Zertifizierungsstellen-zertifikat (hier: *certreply.pem*) und ein privater Schlüssel (hier: *privkey.pem*).

Nach der Ersetzung des Zertifikats auf der Management-Station müssen Sie das Zertifikat auch auf den verwalteten Servern ersetzen (siehe Seite 107 für verwaltete Windows Server oder Seite 109 für verwaltete Linux/VMware Server). Dadurch wird sichergestellt, dass sich die Management-Station weiterhin gegenüber den verwalteten Servern authentisieren kann.

4.2.4.1 Zertifikat auf einem Windows System ersetzen

Gehen Sie wie folgt vor:

1. Stoppen Sie den JBoss Service (siehe Seite 20).
2. Entfernen Sie die Datei *keystore*:
   a) Öffnen Sie die Windows Eingabeaufforderung.
   b) Wechseln Sie in das Verzeichnis <*ServerView directory*>*jboss\standalone\svconf\pki*.
   c) Löschen Sie die *keystore*-Datei oder benennen Sie die Datei um.
3. Kopieren Sie die von der Zertifizierungsstelle signierte Zertifikatsantwort (hier: *certreply.pem*) und das Zertifikat der Zertifizierungsstelle (hier: *certca.pem*) in das aktuelle Verzeichnis (<*ServerView directory*>*jboss\standalone\svconf\pki*).
4. Importieren Sie die Zertifikatsantwort zusammen mit dem Zertifikat der Zertifizierungsstelle in eine neue *keystore*-Datei und exportieren Sie den öffentlichen Schlüssel (hier: *keystore.p12*):

   ```
   openssl pkcs12 -export -chain -in certreply.pem -inkey
   privkey.pem -passout pass:changeit -out keystore.p12
   -name svs_cms -CAfile certca.pem -caname "%CANAME%"
   ```

   Ersetzen Sie den Platzhalter %CANAME% durch den Namen der Zertifizierungsstelle, die die Zertifikatsanforderung (Certificate Signing Request, CSR) signiert hat.
5. Formatieren (reformatieren) Sie die Datei *keystore*:

   ```
   keytool -importkeystore -srckeystore keystore.p12
       -destkeystore keystore -srcstoretype PKCS12
       -srcstorepass changeit -deststorepass changeit
       -destkeypass changeit -srcalias svs_cms
       -destalias svs_cms -noprompt -v
   ```
6. Importieren Sie das neue Zertifikat in die Datei *truststore*.

   Am einfachsten erreichen Sie dies wie folgt:
   a) Starten Sie den JBoss Service.
   b) Warten Sie, bis der Startvorgang beendet ist.
   c) Wechseln Sie in das Verzeichnis <*ServerView directory*>*jboss\standalone\bin*.

d) Öffnen Sie eine Windows Eingabeaufforderung und geben Sie das folgende Kommando / die folgenden Kommandos ein:

```
java -jar install-cert-gui-SVCOM_V1.70.jar
..\svconf\pki\cacerts changeit <system FQDN>:3170
```

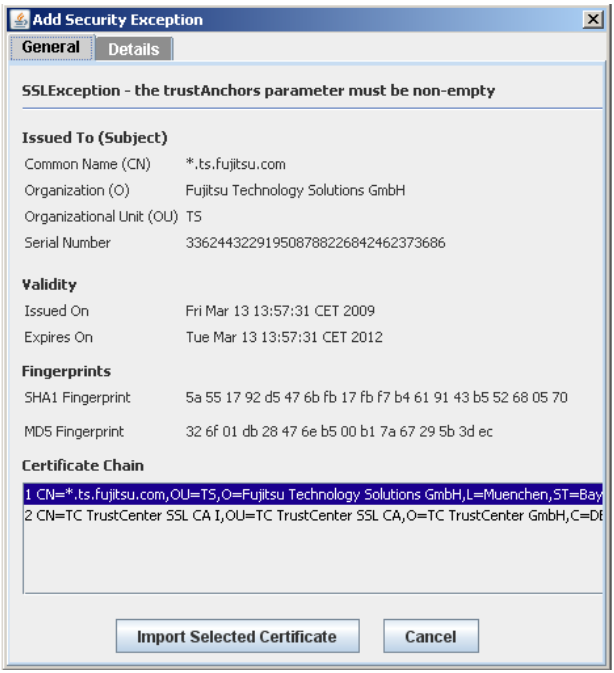
Wenn Sie einen konfigurierten externen Verzeichnisdienst verwenden, **müssen** Sie auch das folgende Kommando eingeben:

```
java -jar install-cert-gui-SVCOM_V1.70.jar
..\svconf\pki\cacerts changeit <system FQDN>:<port>
```

<system FQDN>
: Vollqualifizierter Distinguished Name des betreffenden externen Directory Service-Systems.

<port>
: LDAP-Port, der vom externen Directory Service verwendet wird (meistens: 636).

e) Das Java-Programm *install-cert-gui-SVCOM_V1.70.jar* zeigt einen Bildschirm ähnlich dem folgenden an:


Add Security Exception
General
Details
SSLException - the trustAnchors parameter must be non-empty
Issued To (Subject)
Common Name (CN) *.ts.fujitsu.com
Organization (O) Fujitsu Technology Solutions GmbH
Organizational Unit (OU) TS
Serial Number 336244322919508788226842462373686
Validity
Issued On Fri Mar 13 13:57:31 CET 2009
Expires On Tue Mar 13 13:57:31 CET 2012
Fingerprints
SHA1 Fingerprint 5a 55 17 92 d5 47 6b fb 17 fb f7 b4 61 91 43 b5 52 68 05 70
MD5 Fingerprint 32 6f 01 db 28 47 6e b5 00 b1 7a 67 29 5b 3d ec
Certificate Chain
1 CN=*.ts.fujitsu.com,OU=TS,O=Fujitsu Technology Solutions GmbH,L=Muenchen,ST=Bay
2 CN=TC TrustCenter SSL CA I,OU=TC TrustCenter SSL CA,O=TC TrustCenter GmbH,C=DE
Import Selected Certificate
Cancel
Bild 25: Add Security Exception

In diesem Bildschirm können Sie aus den Zertifikatskette (Certificate Chain) das Zertifikat auswählen, das Sie in die truststore-Datei importieren wollen. Wenn nur ein Eintrag vorhanden ist, ist das Zertifikat selbstsigniert - dann gibt es keine andere Möglichkeit, als dieses Zertifikat zu importieren. Andernfalls werden mindestens zwei Zertifikate angeboten wie im Beispiel gezeigt:

1. Server-Zertifikat.
2. Zertifikat der Zertifizierungsstelle (CA), die das Server-Zertifikat signiert hat.

Im Allgemeinen wird empfohlen, nur das Zertifikat der Zertifizierungsstelle zu importieren. Damit wird jedes andere Server-Zertifikat, das von derselben Zertifizierungsstelle signiert ist, automatisch vertrauenswürdig, was in den meisten Fällen von Vorteil ist.

Nach dem Aufruf des Java-Programms wird die folgende Meldung angezeigt:

```
testConnection(tm,pontresina.servware.abg.firm.net,
3170): SSLException: java.lang.RuntimeException:
Unexpected error:
java.security.InvalidAlgorithmParameterException: the
trustAnchors parameter must be non-empty

writing to truststore ..\svconf\pki\cacerts...
```

Dies bedeutet keinen Fehler, sondern zeigt lediglich an, dass das neue Zertifikat bislang noch nicht in die Datei *truststore* importiert wurde.

f) Erzeugen Sie die Datei *keystore.pem* im PEM-Format.

Gehen Sie wie folgt vor:

- Wechseln Sie zurück in das folgende Verzeichnis:

  <ServerView directory>\jboss\standalone\svconf\pki.

- Wenden Sie das folgende Kommando an:

  ```
  openssl pkcs12 -in keystore.p12 -passin pass:changeit
  -nodes -out keystore.pem -passout pass:
  ```

- Kopieren Sie die Datei *keystore.pem* in das folgende Verzeichnis auf der Management-Station:

  <ServerView directory>\jboss\standalone\svconf\pki.

g) Erzeugen Sie die Datei <*system_name*>.*scs.pem* im PEM-Format.

Gehen Sie wie folgt vor:

- Wenden Sie das folgende Kommando an:

```
openssl pkcs12 -in keystore.p12 -passin pass:changeit -
out <system_name>.scs.pem -passout pass:
```

- Kopieren Sie das erstellte Zertifikat <*system_name*>.*scs.pem* in das folgende Verzeichnis auf der Management-Station:

  <*ServerView directory*>*svcommon\data\download\pki*

  Geben Sie dazu folgendes Kommando ein:

```
COPY <system_name>.scs.pem
"<ServerView directory>\svcommon\data\download\pki\
<system_name>.scs.pem"
```

- Wenn die ServerView-Agenten auf der Management-Station installiert sind:

  Kopieren Sie das erstellte Zertifikat <*system_name*>.*scs.pem* auch in das folgende Verzeichnis auf der Management-Station:

  <ServerView directory>\Remote Connector\pki

  Ein möglicherweise bereits existierendes Zertifikat mit dem selben Namen wird auf der Management-Station ersetzt.

7. Starten Sie den JBoss Service und die ServerView-Dienste neu, um Ihre Änderungen zu aktivieren.

4.2.4.2 Zertifikat auf einem Linux System ersetzen

Gehen Sie wie folgt vor:

1. Stoppen Sie den JBoss Service (siehe Seite 20).
2. Entfernen Sie die Datei *keystore*:
   a) Öffnen Sie ein Terminal, wie z.B. Xterm oder Gnome-term.
   b) Wechseln Sie in das Verzeichnis */opt/fujitsu/ServerViewSuite/jboss/standalone/svconf/pki*.
   c) Löschen Sie die *keystore*-Datei oder benennen Sie die Datei um.
3. Importieren Sie die von der Zertifizierungsstelle signierte Zertifikatsantwort (hier: *certreply.pem*) zusammen mit dem Zertifikat (hier: certca.pem der Zertifizierungsstelle in eine neue *keystore*-Datei und exportieren Sie den öffentlichen Schlüssel (hier: *keystore.p12*):

   ```
   openssl pkcs12 -export -chain -in certreply.pem -inkey
   privkey.pem -passout pass:changeit -out keystore.p12
   -name "svs_cms" -CAfile certca.pem -caname "%CANAME%"
   ```

   Ersetzen Sie den Platzhalter %CANAME% durch den Namen der Zertifizierungsstelle, die die Zertifikatsanforderung (Certificate Signing Request, CSR) signiert hat.
4. Formatieren (reformatieren) Sie die Datei *keystore*:

   ```
   keytool -importkeystore -srckeystore keystore.p12
       -destkeystore keystore -srcstoretype PKCS12
       -srcstorepass changeit -deststorepass changeit
       -destkeypass changeit -srcalias svs_cms
       -destalias svs_cms -noprompt -v
   ```
5. Importieren Sie das neue Zertifikat in die Datei *truststore*.

   Am einfachsten erreichen Sie dies wie folgt:
   a) Starten Sie den JBoss Service.
   b) Warten Sie, bis der Startvorgang beendet ist.
   c) Wechseln Sie in das Verzeichnis *../../bin*.

d) Öffnen Sie ein Terminal-Fenster und geben Sie das folgende Kommando / die folgenden Kommandos ein:

```
java -jar install-cert-gui-SVCOM_V1.70.jar
../conf/pki/cacerts changeit <system FQDN>:3170
```

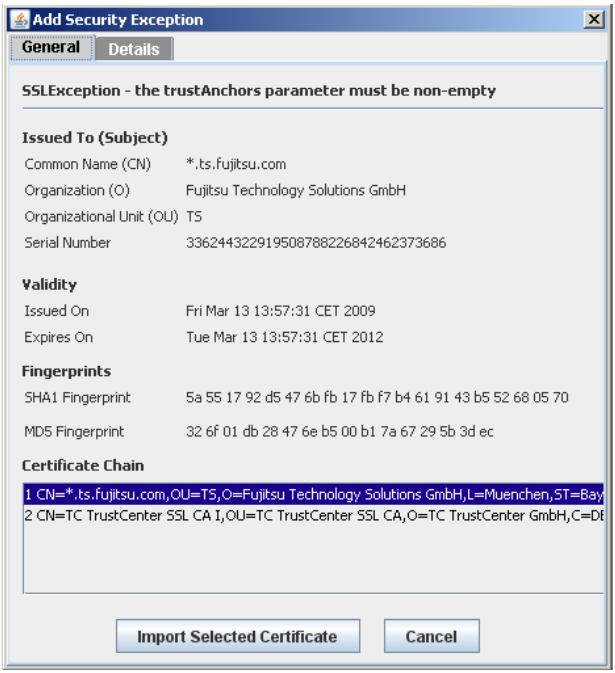
Wenn Sie einen konfigurierten externen Verzeichnisdienst verwenden, **müssen** Sie auch das folgende Kommando eingeben:

```
java -jar install-cert-gui-SVCOM_V1.70.jar
../conf/pki/cacerts changeit <system FQDN>:<port>
```

<system FQDN>
: Vollqualifizierter Distinguished Name des betreffenden Systems.

<port>
: LDAP-Port, der vom externen Directory Service verwendet wird (meistens: 636).

e) Das Java-Programm *install-cert-gui-SVCOM_V1.70.jar* zeigt einen Bildschirm ähnlich dem folgenden an:


Add Security Exception
General
Details
SSLException - the trustAnchors parameter must be non-empty
Issued To (Subject)
Common Name (CN) *.ts.fujitsu.com
Organization (O) Fujitsu Technology Solutions GmbH
Organizational Unit (OU) TS
Serial Number 336244322919508788226842462373686
Validity
Issued On Fri Mar 13 13:57:31 CET 2009
Expires On Tue Mar 13 13:57:31 CET 2012
Fingerprints
SHA1 Fingerprint 5a 55 17 92 d5 47 6b fb 17 fb f7 b4 61 91 43 b5 52 68 05 70
MD5 Fingerprint 32 6f 01 db 28 47 6e b5 00 b1 7a 67 29 5b 3d ec
Certificate Chain
1 CN=*.ts.fujitsu.com,OU=TS,O=Fujitsu Technology Solutions GmbH,L=Muenchen,ST=Bay
2 CN=TC TrustCenter SSL CA I,OU=TC TrustCenter SSL CA,O=TC TrustCenter GmbH,C=DE
Import Selected Certificate
Cancel
Bild 26: Add Security Exception

In diesem Bildschirm können Sie aus den Zertifikatskette (Certificate Chain) das Zertifikat auswählen, das Sie in die truststore-Datei importieren wollen. Wenn nur ein Eintrag vorhanden ist, ist das Zertifikat selbstsigniert - dann gibt es keine andere Möglichkeit, als dieses Zertifikat zu importieren. Andernfalls werden mindestens zwei Zertifikate angeboten wie im Beispiel gezeigt:

1. Server-Zertifikat.
2. Zertifikat der Zertifizierungsstelle (CA), die das Server-Zertifikat signiert hat.

Im Allgemeinen wird empfohlen, nur das Zertifikat der Zertifizierungsstelle zu importieren. Damit wird jedes andere Server-Zertifikat, das von derselben Zertifizierungsstelle signiert ist, automatisch vertrauenswürdig, was in den meisten Fällen von Vorteil ist.

Nach dem Aufruf des Java-Programms wird die folgende Meldung angezeigt:

```
testConnection(tm,pontresina.servware.abg.firm.net,
3170): SSLException: java.lang.RuntimeException:
Unexpected error:
java.security.InvalidAlgorithmParameterException: the
trustAnchors parameter must be non-empty

writing to truststore ..\svconf\pki\cacerts...
```

Dies bedeutet keinen Fehler, sondern zeigt lediglich an, dass das neue Zertifikat bislang noch nicht in die Datei *truststore* importiert wurde.

f) Erzeugen Sie die Datei *keystore.pem* im PEM-Format.

Gehen Sie wie folgt vor:

- Wenden Sie das folgende Kommando an:

```
openssl pkcs12 -in keystore.p12 -passin pass:changeit
-nodes -out keystore.pem -passout pass:changeit
```

- Öffnen Sie die Datei *keystore.pem* mit einem Text-Editor und löschen Sie alle Textzeilen mit Ausnahme der folgenden Zeilen:
  - Kopf- und Fußzeilen, die mit "-----" markiert sind.
  - Verschlüsselte Zeilen in Datenblöcken.
- Kopieren Sie die Datei *keystore.pem* in das folgende Verzeichnis auf der Management-Station:

  /opt/fujitsu/ServerViewSuite/jboss/standalone/svconf/pki

g) Kopieren Sie das Zertifikat der Zertifizierungsstelle im Format <*system_name*>.*scs.pem* in in das folgende Verzeichnis auf der Management-Station:

/opt/fujitsu/ServerViewSuite/svcommon/data/download/pki

Gehen Sie wie folgt vor:

- Wenden Sie das folgende Kommando an:

```
cp certca.pem
/opt/fujitsu/ServerViewSuite/svcommon/data/download/pki/
<system_name>.scs.pem
```

6. Starten Sie den JBoss Service neu, um Ihre Änderungen zu aktivieren.

4.3 Verwalteten Server Systeme für Role Based Access (RBAC) und Client-Authentifizierung einrichten

Die Einrichtung eines verwalteten Servers (Managed Node) für RBAC und Client-Authentifizierung erfordert die folgenden Schritte:

1. Zertifikatsdateien (<*system_name*>.*scs.pem*) und <*system_name*>.*scs.xml*) auf den verwalteten Server übertragen.
2. Übertragene Dateien auf dem verwalteten Server installieren.

4.3.1 Dateien <system_name>.scs.pem und <system_name>.scs.xml auf den verwalteten Server übertragen

Nach erfolgreicher Installation des Operation Managers auf der Management-Station finden Sie die Dateien <*system_name*>.*scs.pem* und <*system_name*>.*scs.xml* auf der Management-Station im folgenden Verzeichnis:

– <*ServerView directory*>*svcommon\data\download\pki* (auf Windows Systemen)

– */opt/fujitsu/ServerViewSuite/svcommon/data/download/pki* (auf Linux Systemen)

Sie können die Dateien „manuell“ auf den verwalteten Server übertragen oder - komfortabler - von der Management-Station herunter laden.

Voraussetzungen für das Herunterladen der Dateien:

Sie müssen die Administrator-Rolle besitzen.

Zum Herunterladen der Dateien gehen Sie wie folgt vor:

1. Geben Sie am Browser des verwalteten Servers die folgende URL ein:

   https://<system_name>:3170/Download/pki/

   Wichtig:

   Die URL muss mit einem Schrägstrich, Slash (/), abschließen.

   <system_name>

   Für *<system_name>* tragen Sie den DNS-Namen oder die IP-Adresse der Management-Station ein.

   Es öffnet sich das folgende Fenster, das die Dateien als „bereit zum Herunterladen“ anzeigt.

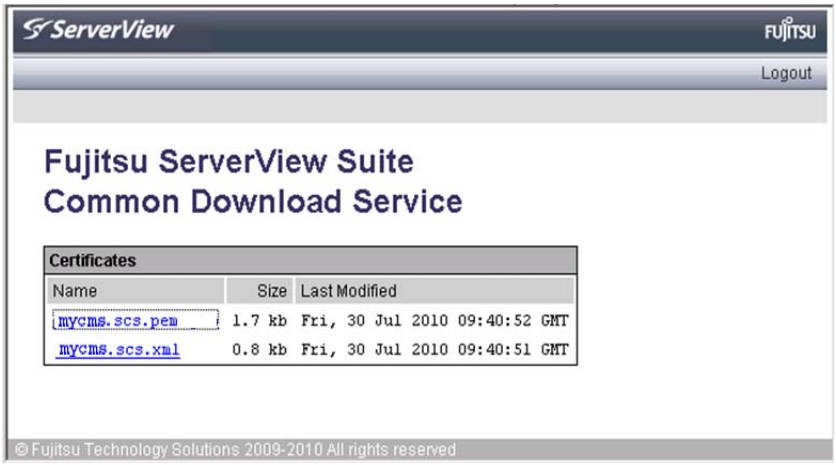


Bild 27: Dateien mycms.scs.pem und mycms.scs.xml von der zentralen Management-Station mycms herunterladen

2. Klicken Sie für jede der beiden Dateien mit der rechten Maustaste auf den zugehörigen Link, und speichern Sie die Datei mit *Save target as...* auf dem verwalteten Server.

   Save target as ... speichert die *.pem*-Datei möglicherweise als *.html*-Datei. IÄndern Sie in diesem Fall das Suffix *.html* in *.pem* um sicherzustellen, dass die Datei verwendet wird.

4.3.2 Zertifikatsdateien auf einem Windows System installieren

Zur Installation der Zertifikatsdateien <*system_name*>.*scs.pem* und <*system_name*>.*scs.xml* stehen Ihnen die beiden folgenden Möglichkeiten zur Verfügung::

– Zertifikatsdateien gleich zu Beginn zusammen mit den ServerView-Agenten auf dem verwalteten Server installieren.

– Zertifikatsdateien auf einem verwalteten Server installieren, auf dem die ServerView-Agenten bereits installiert sind.Dieses Vorgehen ist z.B. zu wählen, wenn das zunächst installierte selbstsignierte Zertifikat durch das Zertifikat einer vertrauenswürdigen Zertifizierungsstelle ersetzt werden muss (z.B. als Folge eines entsprechenden Zertifikatsaustauschs auf der Management-Station).

4.3.2.1 Zertifikatsdateien gemeinsam mit den ServerView Agenten installieren

In diesem Fall müssen die Zertifikatsdateien auf dem verwalteten Server installiert sein, bevor die ServerView Agenten installiert werden.

Im Folgenden ist beschrieben, wie Sie die Zertifikatsdateien auf einem Windows System installieren. Einzelheiten zur Installation der ServerView-Agenten finden Sie in den entsprechenden Abschnitten des Handbuchs „ServerView-Agenten für Windows“.

Installieren via Paket-Installation

Gehen Sie wie folgt vor:

1. Kopieren Sie die gepackte Setup-Datei (*ServerViewAgents_Win_i386.exe* oder*ServerViewAgents_Win_x64.exe*) für das Agenten-Setup auf ein freigegebenes Netzlaufwerk oder in ein lokales Verzeichnis auf dem verwalteten Server.
2. Im Verzeichnis, das die Setup-Datei enthält: Erstellen Sie ein neues Verzeichnis *pki* (Abkürzung für "public key infrastructure").
3. Transferieren Sie die Zertifikatsdateien <*system_name*>.*scs.pem* und <*system_name*>.*scs.xml* in das neue Verzeichnis *pki*. Dabei können Sie auch gleichzeitig die Zertifikatsdateien mehrerer vertrauenswürdiger Management-Stationen übertragen.

4. Starten Sie die Paket-Installation (siehe Handbuch „ServerView-Agenten für Windows“).

   Alle Zertifikate im Verzeichnis *pki* werden bei der Installation der ServerView-Agenten an geeigneter Stelle installiert.

Installieren via entpackter Installation

Gehen Sie wie folgt vor:

1. Entpacken Sie die Setup-Dateien *ServerViewAgents_Win_i386.exe* oder *ServerViewAgents_Win_x64.exe* auf ein freigegebenes Netzlaufwerk oder in ein lokales Verzeichnis auf dem verwalteten Server.

   Dabei werden die Dateien *Setup.exe*, *ServerViewAgents_xxx.msi* und andere Dateien erzeugt.

2. Im Verzeichnis, das die Setup-Dateien enthält: Erstellen Sie ein neues Verzeichnis *pki* (Abkürzung für "public key infrastructure").

3. Transferieren Sie die Zertifikatsdateien <*system_name*>*.scs.pem* und <*system_name*>*.scs.xml* in das neue Verzeichnis *pki*. Dabei können Sie auch gleichzeitig die Zertifikatsdateien mehrerer vertrauenswürdiger Management-Stationen übertragen.

4. Starten Sie *Setup.exe* (siehe Handbuch "ServerView-Agenten für Windows").

   Alle Zertifikate im Verzeichnis *pki* werden bei der Installation der ServerView-Agenten an geeigneter Stelle installiert.

Installieren via ServerView Suite DVD

ServerView-Agenten und Zertifikate können nicht direkt von der ServerView Suite DVD installiert werden.

Gehen Sie wie folgt vor:

1. Kopieren Sie die gepackte oder entpackten Setup-Dateien auf ein freigegebenes Netzlaufwerk oder in ein lokales Verzeichnis auf dem verwalteten Server.

2. Im Verzeichnis, das die Setup-Datei(en) enthält: Erstellen Sie ein neues Verzeichnis *pki* (Abkürzung für "public key infrastructure").

3. Transferieren Sie die Zertifikatsdateien <*system_name*>*.scs.pem* und <*system_name*>*.scs.xml* in das neue Verzeichnis *pki*. Dabei können Sie auch gleichzeitig die Zertifikatsdateien mehrerer vertrauenswürdiger Management-Stationen übertragen.

4. Starten Sie die Paket-Installation (siehe Handbuch „ServerView-Agenten für Windows“).

   Alle Zertifikate im Verzeichnis *pki* werden bei der Installation der ServerView-Agenten an geeigneter Stelle installiert.

4.3.2.2 Zertifikat auf einem Windows System installieren, auf dem die Windows-Agenten bereits installiert sind

Gehen Sie wie folgt vor:

1. Finden Sie den Pfad (im Folgenden kurz: <*scsPath*>) des ServerView Remote Connector Service (SCS) auf dem verwalteten Server.

   Voreingestellt ist der folgende Pfad:

   – Für x64 Systeme:

   C:\Program Files (x86)\Fujitsu\ServerView Suite\Remote Connector

   – Für i386 Systeme:

   C:\Program Files\Fujitsu\ServerView Suite\Remote Connector

2. Transferieren Sie die Dateien <*system_name*>*.scs.pem* und <*system_name*>*.scs.xml* in den SCS Zertifikatordner <*scsPath*>*pki*.

   Nach einem Neustart des Remote Connector Service werden die neuen oder ausgetauschten Zertifikate innerhalb von 10 Sekunden neu geladen.

4.3.3 Zertifikatsdateien auf einem Linux oder VMware System installieren

Zur Installation der Zertifikatsdateien *<system_name>.scs.pem* und *<system_name>.scs.xml* stehen Ihnen die beiden folgenden Möglichkeiten zur Verfügung::

– Zertifikatsdateien gleich zu Beginn zusammen mit den ServerView-Agenten auf dem verwalteten Server installieren.

– Zertifikatsdateien auf einem verwalteten Server installieren, auf dem die ServerView-Agenten bereits installiert sind.Dieses Vorgehen ist z.B. zu wählen, wenn das zunächst installierte selbstsignierte Zertifikat durch das Zertifikat einer vertrauenswürdigen Zertifizierungsstelle ersetzt werden muss (als Folge eines entsprechenden Zertifikatsaustauschs auf der Management-Station.

4.3.3.1 Zertifikatsdateien gemeinsam mit den ServerView Agenten installieren

In diesem Fall müssen die Zertifikatsdateien auf dem verwalteten Server installiert sein, **bevor** die ServerView-Agenten installiert werden.

Im Folgenden ist beschrieben, wie Sie die Zertifikatsdateien auf einem Linux/VMware System installieren. Einzelheiten zur Installation der ServerView Agenten finden Sie in den entsprechenden Abschnitten des Handbuchs „ServerView-Agenten für Linux“.

Installieren via ServerView Suite DVD

1. Kopieren Sie die Dateien <*system_name*>.*scs.pem* und <*system_name*>.*scs.xml* in das */temp* -Verzeichnis.
2. Exportieren Sie die Umgebungsvariable *SV_SCS_INSTALL_TRUSTED* durch Eingabe des Kommandos

   ```
   export SV_SCS_INSTALL_TRUSTED=/tmp
   ```

3. Geben Sie folgendes Kommando ein:

   ```
   sh srvmagtDVD.sh [-R]
   ```

   Die Zertifikatsdateien <*system_name*>.*scs.pem* und <*system_name*>.*scs.xml* werden importiert.

   Nach einem Neustart des Remote Connector Service werden die neuen oder ausgetauschten Zertifikate innerhalb von 10 Sekunden neu geladen.

Installieren aus einem Verzeichnis

1. Transferieren Sie die Dateien <*system_name*>.*scs.pem* und <*system_name*>.*scs.xml* in das lokale Verzeichnis, das die Module der ServerView-Agenten enthält.
2. Geben Sie folgendes Kommando ein:

   ```
   sh ./srvmagt.sh [option] install
   ```

   Die Zertifikatsdateien <*system_name*>.*scs.pem* und <*system_name*>.*scs.xml* werden importiert.

Installieren mit dem rpm-Kommando

1. Transferieren Sie die Dateien <*system_name*>.*scs.pem* und <*system_name*>.*scs.xml* in ein lokales Verzeichnis <*cert dir*>.
2. Exportieren Sie die Umgebungsvariable *SV_SCS_INSTALL_TRUSTED* durch Eingabe des Kommandos

   ```
   export SV_SCS_INSTALL_TRUSTED=<cert dir>
   ```

3. Geben Sie folgendes Kommando ein:

   ```
   rpm -U ServerViewConnectorService-<scs-version>.i386.rpm
   ```

   Die Zertifikatsdateien <*system_name*>.*scs.pem* und <*system_name*>.*scs.xml* werden importiert.

4.3.3.2 Zertifikat auf einem Linux/VMware System installieren, auf dem die ServerView-Agenten bereits installiert sind

Gehen Sie wie folgt vor:

1. Starten Sie ein Terminal (mit *root*-Berechtigung).
2. Finden Sie den Pfad (im Folgenden kurz: <*scsPath*>) des ServerView Remote Connector Service (SCS) auf dem verwalteten Server.

   Voreingestellt ist der folgende Pfad:

   /opt/fujitsu/ServerViewSuite/SCS/pki
3. Transferieren Sie die Dateien <*system_name*>*.scs.pem* und <*system_name*>*.scs.xml* in ein lokales Verzeichnis.
4. Geben Sie das folgende Kommando ein:

   ```
   cp -p <system_name>.scs.pem <system_name>.scs.xml <scsPath>
   ```

   Nach einem Neustart des Remote Connector Service werden die neuen oder ausgetauschten Zertifikate innerhalb von 10 Sekunden neu geladen.

4.3.4 Zertifikat via ServerView Update Manager installieren (auf einem Windows / Linux / VMware System)

Voraussetzungen:

Der ServerView-Update-Agent und die ServerView-Agenten müssen mindestens Version 5.0 vorliegen.

Für jeden in der Serverliste angezeigten verwalteten Server bietet der Update-Mechanismus des ServerView Update Managers die Möglichkeit, das Zertifikat der Management-Station (im Folgenden kurz: CMS-Zertifikat) direkt aus der Serverliste heraus auf dem verwalteten Server zu installieren. Wie andere Update-Komponenten auch, bietet Ihnen der Update Manager das CMS-Zertifikat als zu installierende Software an. Durch Generieren und Starten eines entsprechenden Update-Jobs können Sie das Zertifikat automatisch zum verwalteten Server übertragen.

Hierzu muss jede für die Management-Station erstellte Zertifikatsdatei im Repository des Update Managers enthalten sein (Pfadname: *...\Tools\Certificates* (Windows) und *.../Tools/Certificates* (Linux / VMware):

– Bei der regulären Erstinstallation des Repository fügt der Konfigurationsassistent des Update Managers die Zertifikate am Ende der Konfigurationsphase zum Repository hinzu.

– Während einer Update-Installation werden die Zertifikate durch Ausführung der entsprechenden Installations-Skripts automatisch zum Repository hinzugefügt.

Wichtig!

Es darf nur ein lokales Repository angegeben werden, da die hinzugefügten Daten ausschließlich für die betreffende Management-Station gültig sind.

4.3.4.1 Mit dem ServerView Update Manager das CMS-Zertifikat auf dem verwalteten Server installieren (Überblick)

Die Installation des CMS-Zertifikats können Sie über das Update Manager-Hauptfenster gemäß der nachfolgenden Beschreibung steuern.

Einzelheiten zum ServerView Update Manager finden Sie im Handbuch „ServerView Update Manager“.

Server Details im Hauptfenster des Update Managers (vor Installation des CMS-Zertifikats auf dem verwalteten Server)

Solange das CMS-Zertifikat noch nicht auf dem verwalteten Server installiert ist, wird unter *Agent Access* in der Registerkarte *Server Details* der Hinweis "not certified" angezeigt (siehe Bild 28).

Sofern nicht sowohl der ServerView Update-Agent als auch die ServerView Agenten mindestens von der Version 5.0 sind, wird für den betreffenden Servern unter *Agent Access* in der Registerkarte *Server Details* der Hinweis "restricted" oder "unrestricted" angezeigt.

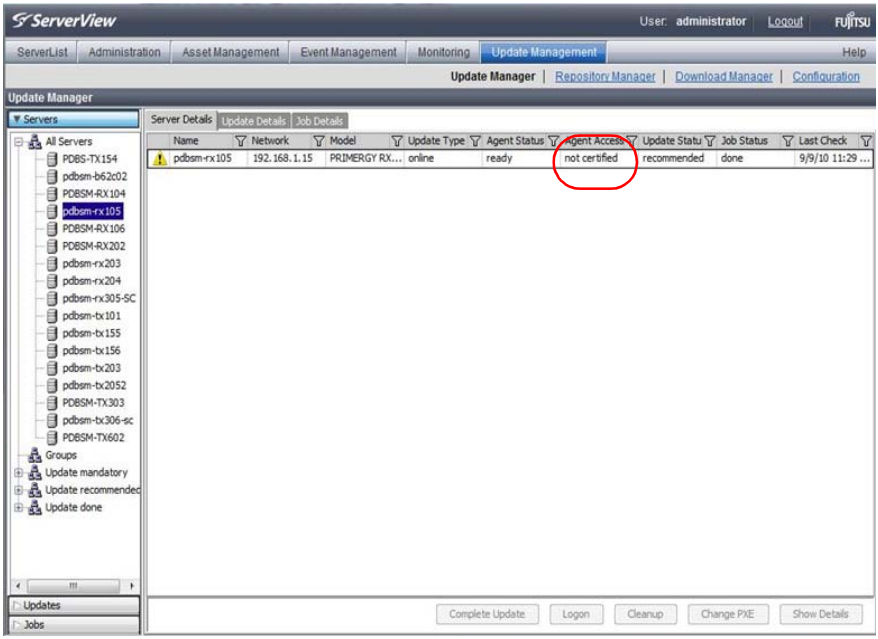


Bild 28: Update Manager Hauptfenster - Registerkarte Server Details (CMS-Zertifikat ist noch nicht installiert.)

Update Details im Hauptfenster des Update Managers (vor Installation des CMS-Zertifikats auf dem verwalteten Server)

Eine separate Zeile in der Ansicht *Upgrades* der Registerkarte *Update Details* informiert über die Möglichkeit, das CMS-Zertifikat auf dem ausgewählten Server zu installieren (siehe Bild 29).

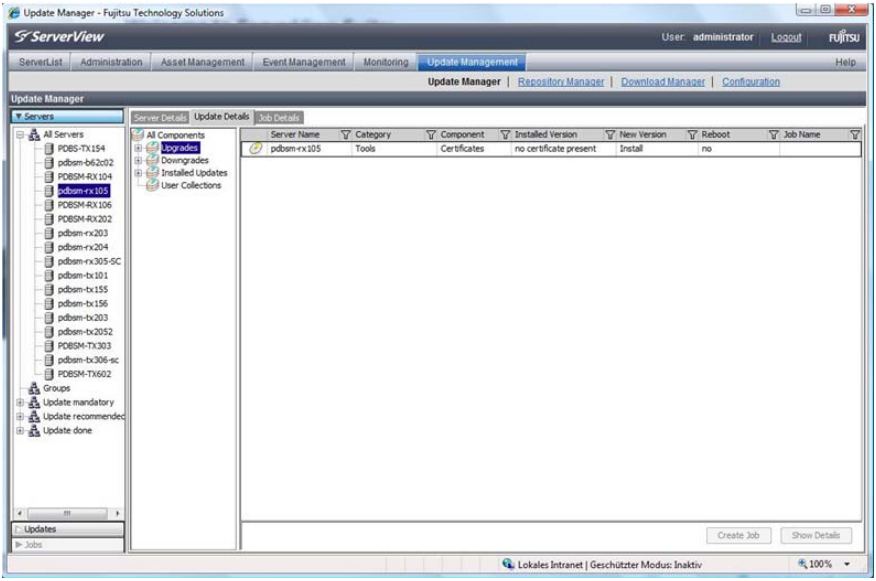


Bild 29: Update Manager Hauptfenster - Registerkarte Update Details (CMS-Zertifikat ist noch nicht installiert)

Nun können Sie einen Update-Job erzeugen und starten, der die Installation auf dem verwalteten Server durchführt. Optional kann der Update-Job zusätzliche Update-Komponenten umfassen. Einzelheiten zum Erstellen eines Update-Jobs finden Sie im Handbuch „ServerView Update Manager“.

Server Details im Hauptfenster des Update Managers (nach erfolgreicher Installation des CMS-Zertifikats auf dem verwalteten Server)

Sobald das CMS-Zertifikat auf dem verwalteten Server erfolgreich installiert ist, wird für diesen Server unter *Agent Access* in der Registerkarte *Server Details* der Hinweis "certified" angezeigt (siehe Bild 30).

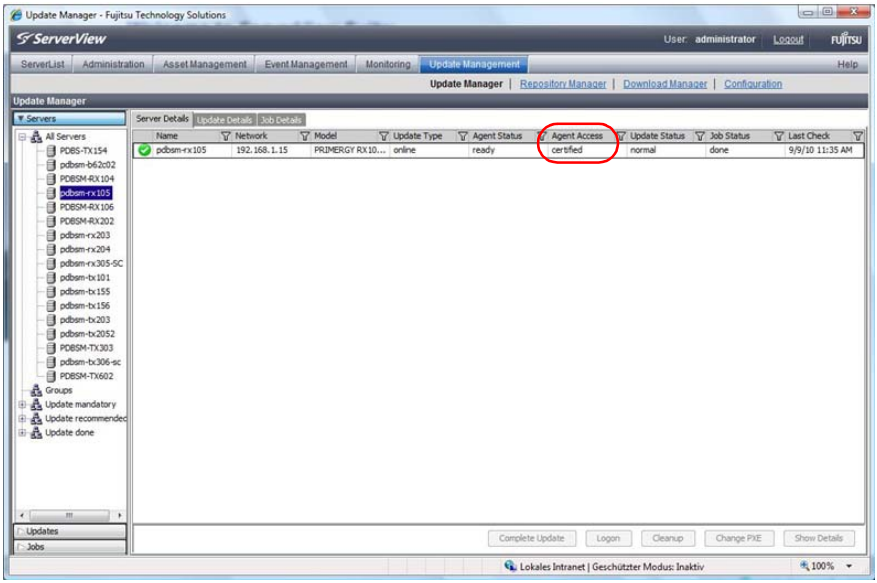


Bild 30: Update Manager Hauptfenster - Registerkarte Server Details (CMS-Zertifikat wurde erfolgreich installiert.)

Update Details im Hauptfenster des Update Managers (nach erfolgreicher Installation des CMS-Zertifikats auf dem verwalteten Server)

Sobald das CMS-Zertifikat auf dem verwalteten Server erfolgreich installiert ist, informiert eine separate Zeile in der Ansicht *Installed Updates* der Registerkarte *Update Details* über die erfolgreiche Installation des CMS-Zertifikats auf dem verwalteten Server (siehe Bild 31).

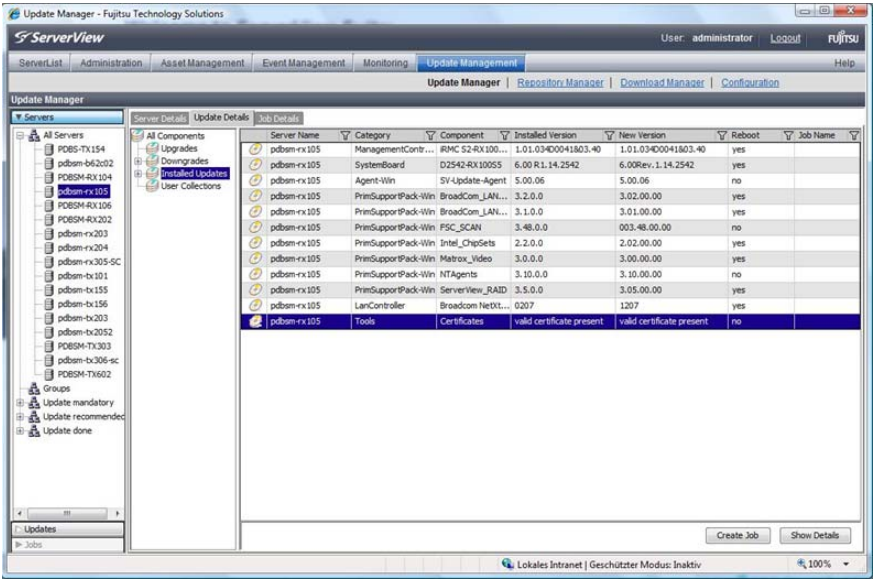


Bild 31: Update Manager Hauptfenster - Registerkarte Update Details (CMS-Zertifikat erfolgreich installiert)

4.3.4.2 CMS-Zertifikat auf dem verwalteten Server installieren

Zur Installation des CMS-Zertifikats auf dem verwalteten Server gehen Sie wie folgt vor:

1. Öffnen Sie das Hauptfenster des *Update Managers* (siehe Bild 28).
2. Wählen Sie unter *All Servers,* den verwalteten Server aus, auf dem Sie das CMS-Zertifikat installieren wollen.
3. Wählen Sie in der Ansicht *Upgrades* der Registerkarte *Update Details* (siehe Bild 29) die Zeile aus, die die Option zum Installieren des CMS-Zertifikats auf dem ausgewählten Server anzeigt.
4. Erzeugen und starten Sie einen neuen Update-Job, der das CMS-Zertifikat auf dem verwalteten Server installiert.

4.3.4.3 CMS-Zertifikat auf dem verwalteten Server deinstallieren

Zur Deinstallation des CMS-Zertifikats auf dem verwalteten Server gehen Sie wie folgt vor:

1. Öffnen Sie das Hauptfenster des *Update Managers* (siehe Bild 28).
2. Wählen Sie unter *All Servers,* den verwalteten Server, auf dem Sie das CMS-Zertifikat deinstallieren wollen.
3. Wählen Sie in der Ansicht *Downgrades* der Registerkarte *Update Details* die Zeile aus, die in der Spalte *New Version* "Unstinstall" anzeigt (siehe Bild 32 auf Seite 116).
4. Erzeugen und starten Sie einen neuen Update-Job, der das CMS-Zertifikat auf dem verwalteten Server deinstalliert.

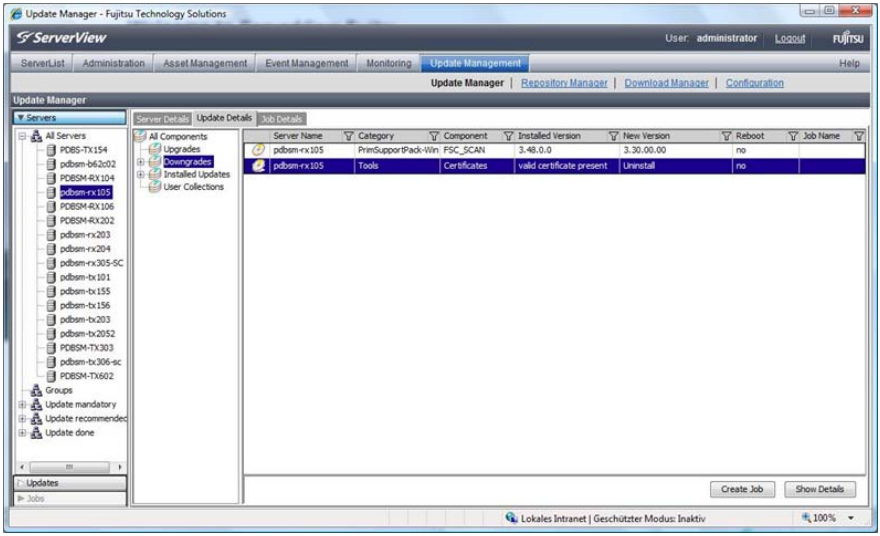


Bild 32: Update Manager Hauptfenster - Update Details (Ansicht Downgrades)

5 Rollenbasierte Berechtigungen für den Zugriff auf den Operations Manager

Rollenbasierte Zugangskontrolle (Role-Based Access Control, RBAC) regelt die Benutzer-Authentifizierung durch Zuweisung von Berechtigungen (Privilegien) auf der Basis von Benutzerrollen (User Roles, Security Roles). Mit jeder Rolle können Sie ein spezifisches, aufgabenorientiertes Berechtigungsprofil definieren.

Die RBAC-Implementation der ServerView Suite gruppiert Berechtigungen in Kategorien, die sich jeweils auf eine spezielle ServerView-Komponente beziehen.

Dieses Kapitel erläutert die folgenden Themen:

– Alle Kategorien und die zugehörigen Berechtigungen (Privilegien)

– Vordefinierten Rollen *Administrator*, *Monitor, Operator* und *UserAdministrator* und zugehörige Berechtigungen.

5.1 Privilegien-Kategorien und zugehörige Berechtigungen

Die Berechtigungen, die zur Nutzung der einzelnen ServerView-Komponenten oder zur Ausführung ServerView-spezifischer Aufgaben berechtigen, sind in Privilegien-Kategorien (kurz: Kategorien) gruppiert.

Jede Kategorie bezieht sich auf eine spezifische ServerView-Komponente und umfasst alle Berechtigungen, die Sie berechtigen, die zugehörige ServerView-Komponente zu nutzen oder eine Komponenten-spezifische Aufgabe durchzuführen.

5.1.1 Privilegien-Kategorien (Überblick)

Die ServerView Suite kennt die folgenden Privilegien-Kategorien:

Privilegien-Kategorie	**Zugehörige ServerView-Komponente / Aufgabe**
AgentDeploy	Installation der ServerView-Agenten
AlarmMgr	Alarm-Management
ArchiveMgr	Archive Manager
BackupMgr	Sicherung der ServerView-Datenbank
Common	Allgemeine ServerView Suite-spezifische Berechtigungen
ConfigMgr	Server Configuration Manager (SCU) und ferngesteuerte Energieverwaltung (Remote Power Management)
InvMgr	Inventory Manager
iRMC_MMB	iRMC S2/S3/S4 / BladeServer-MMB)
PerfMgr	Performance Manager und Threshold Manager
PowerMon	Power Monitor
RackManager	Rack Manager
RaidMgr	RAID Manager
RemDeploy	Deployment Manager und Installation Manager
ReportMgr	Wird nur noch aus Kompatibilitätsgründen unterstützt.
SCS	ServerView Connector Service
ServerList	Serverliste
UpdMgr	Update Manager

Table 4: Privilegien-Kategorien und zugehörige ServerView-Komponenten/Aufgaben

Privilegien-Kategorie	Zugehörige ServerView-Komponente / Aufgabe
UserMgr	Benutzerverwaltung mit OpenDJ
VIOM	Virtual-IO Manager

Table 4: Privilegien-Kategorien und zugehörige ServerView-Komponenten/Aufgaben

5.1.2 Kategorie AgentDeploy

Die *PerformAgentDeployment*-Berechtigung der *AgentDeploy*-Kategorie wird benötigt, um ServerView-Agenten auf Managed Nodes zu installieren.

Privileg	Erlaubnis	Geltungsbereich
PerformAgentDeployment	ServerView- Agenten auf Managed Nodes einrichten	Management-Station

Table 5: Berechtigung der Kategorie AgentDeploy

5.1.3 Kategorie AlarmMgr

Die *AlarmMgr*-Kategorie umfasst die Berechtigungen zur Ausführung der verschiedenen Aufgaben in Verbindung mit dem ServerView Event-Management.

Privileg	Erlaubnis	Geltungsbereich
AccessAlarmMgr	Zugriff auf den Alarm Monitor.	Management-Station
ModifyAlarmConfig	Alarmeinstellungen modifizieren mithilfe des *Alarm Configuration*-Links im Startfenster des Operations Managers. **Hinweis:** Diese Berechtigung sollte nur an Benutzer vergeben werden, die bereits die *AccessServerList*-Berechtigung besitzen.	Management-Station
PerformAlarmAcknowledge	Alarme bestätigen.	Alle
PerformMIBIntegration	Neue MIBs integrieren.	Managed Node

Table 6: Berechtigung der Kategorie AlarmMgr

5.1.4 Kategorie ArchiveMgr

Die *ArchiveMgr*-Kategorie umfasst die Berechtigungen für den Zugriff auf den Archive Manager sowie für das Erzeugen, Ändern und Löschen von Archiven.

Berechtigung	Erlaubnis	Geltungsbereich
AccessArchiveMgr	Zugriff auf den Archive Manager.	Management-Station
ModifyArchives	Archive erzeugen, ändern und löschen	Management-Station

Table 7: Berechtigungen der Kategorie ArchiveMgr

5.1.5 Kategorie BackupMgr

Die *BackupMgr*-Kategorie umfasst die Berechtigungen für die Verwaltung von Sicherungskopien der ServerView-Datenbank .

Berechtigung	Erlaubnis	Geltungsbereich
ModifyBackup	Sicherungskopie der ServerView-Datenbank erzeugen/löschen.	Management-Station
PerformBackupRestore	ServerView-Datenbank wiederherstellen.	Management-Station
PerformBackupTransfer	Sicherungskopie der ServerView-Datenbank erzeugen/löschen.	Management-Station

Table 8: Berechtigungen der Kategorie BackupMgr

5.1.6 Kategorie Common

Die Kategorie *Common* umfasst die Berechtigungen für die Ausführung allgemeiner ServerView-spezifischer Aufgaben.

Berechtigung	Erlaubnis	Geltungsbereich
AccessOnlineDiagnostics	Online Diagnostics auf einem Managed Node ausführen.	Managed Node
AccessPrimeCollect	PrimeCollect auf einem Managed Node ausführen.	Managed Node
AccessRemoteManagement	Komponenten für das Remote Management ausführen.	Alle
ConfigPKI	Keystore oder Truststore modifizieren, d.h. Berechtigung für den Import und Export von Zertifikaten.	Alle
ModifyCMSSettings	Lokale Konfigurtionseinstellungen auf der Management-Station ändern.	Alle
ModifyPasswordTable	Passwort-Tabelle ändern.	Management-Station
PerformDownload	Daten aus dem ServerView Installationsverzeichnis auf die Management-Station herunterladen.	Management-Station
PerformLocateToggle	Identifizierungs-LED ein-/ausschalten	Managed Node
PerformServerErrorAck	Fehlermeldung bezüglich eines Servers bestätigen.	Management-Station

Table 9: Berechtigungen der Kategorie Common

5.1.7 Kategorie ConfigMgr

Die *ConfigMgr*-Kategorie umfasst die Berechtigungen für Zugriff auf und Benutzung des Server Configuration Managers sowie die Berechtigungen zur Nutzung der Funktionalität des Operations Managers für die ferngesteuerte Energieverwaltung (Remote Power Management).

Berechtigung	Erlaubnis	Geltungsbereich
AccessServerConfig	Zugriff auf den Server Configuration Manager.	Alle
ModifyPowerOnOffSettings	Shutdown-Kommandos ausführen und Shutdown-Einstellungen ändern.	Alle
ModifyServerConfig	Server-Konfiguration von Managed Nodes mithilfe des Server Configuration Managers ändern.	Alle

Table 10: Berechtigungen der Kategorie ConfigMgr

5.1.8 Kategorie InvMgr

Die *InvMgr* -Kategorie umfasst die Berechtigungen für den Zugriff auf den Inventory Manager und für das Erzeugen / Ändern / Löschen / Ausführen DataCollections und Reports.

Berechtigung	Erlaubnis	Geltungsbereich
AccessInvMgr	Zugriff auf Inventory Manager.	Management-Station
ModifyCollections	DataCollections und zugehörige Definitionen erzeugen, ändern und löschen.	Management-Station
ModifyDiagnostics	Task-spezifisches Logging ansehen / löschen und Daten exportieren.	Management-Station
ModifyReports	DataCollections und zugehörige Definitionen erzeugen, ändern und löschen.	Management-Station
PerformCollections	DataCollections durchführen.	Management-Station
PerformReports	Reports durchführen.	Management-Station

Table 11: Berechtigungen der Kategorie InvMgr

5.1.9 Kategorie iRMC_MMB

Die *iRMC_MMB* -Kategorie umfasst die Berechtigungen für Zugriff auf und Nutzung von iRMC S2/S3/S4 / MMB.

Wichtiger Hinweis:

Berechtigungen mit dem Präfix "Ipmi" basieren auf den in der IPMI Specification spezifizierten Berechtigungen. Im IPMI-Standard ist die Benutzerkonfiguration kanalspezifisch. Benutzer können für den Zugriff auf iRMC S2/S3/S4 / MMB unterschiedliche Berechtigungsprofile besitzen, je nachdem ob sie via LAN-Kanal oder via seriellem Kanal zugreifen.

Für jeden Benutzer / Rolle muss genau ein IpmiLan Privilege Level und ein Ipmi Serial Privilege Level spezifiziert werden.

Berechtigung	Erlaubnis	Geltungsbereich
CfgConnectionBlade	Erlaubnis zur Konfiguration des Connection Blade.	Managed Node
IpmiLanOem	OEM-spezifischer IPMI Privilege Level *OEM* für alle LAN-Verbindungen. Der *OEM*-Level umfasst den Standard IPMI Privilege Level *administrator* und gestattet darüber hinaus die Ausführung von OEM-Funktionen.	Managed Node
IpmiLanOperator	Standard IPMI Privilege Level *operator* für alle LAN-Verbindungen.	Managed Node
IpmiLanUser	Standard IPMI Privilege Level *user* für alle LAN-Verbindungen.	Managed Node
IpmiSerialOem	OEM-specifischer IPMI Privilege Level *OEM* für alle LAN-Verbindungen. Der *OEM*-Level umfasst den Standard IPMI Privilege Level *administrator* und gestattet darüber hinaus die Ausführung von OEM-Funktionen.	Managed Node
IpmiSerialOperator	Standard IPMI Privilege Level *operator* für alle LAN-Verbindungen.	Managed Node
IpmiSerialUser	Standard IPMI Privilege Level *user* für alle LAN-Verbindungen.	Managed Node

Table 12: Berechtigungen der Kategorie iRMC_MMB

Berechtigung	Erlaubnis	Geltungsbereich
iRMCsettings	Erlaubnis zum Ändern der iRMC S2/S3/S4-Einstellungen (Konfiguration)	Managed Node
RemoteStorage	Erlaubnis zur Nutzung der *Remote Storage*-Funktionalität des iRMC S2/S3/S4.	Managed Node
UserAccounts	Erlaubnis zum Erzeugen, Löschen und Ändern von Benutzerkennungen im lokalen Speicher des iRMC S2/S3/S4 / MMB.	Managed Node
VideoRedirection	Erlaubnis zum Öffnen einer AVR-Sitzung (Konsolen-Umleitung) via iRMC S2/S3/S4.	Managed Node

Table 12: Berechtigungen der Kategorie iRMC_MMB

5.1.10 Kategorie PerfMgr

Die *PerfMgr* -Kategorie umfasst die Berechtigungen für Zugriff auf und Nutzung von Performance Manager und Threshold Manager.

Berechtigung	Erlaubnis	Geltungsbereich
AccessPerformanceMgr	Zugriff auf den Performance Manager.	Management-Station
AccessThresholdMgr	Zugriff auf Threshold Manager **Hinweis:** Diese Berechtigung sollte nur an Benutzer vergeben werden, die bereits die *AccessServerList*-Berechtigung besitzen.	Management-Station

Table 13: Berechtigungen der Kategorie PerfMgr

5.1.11 Kategorie PowerMon

Die *AccessPowerMonitor*-Berechtigung der *PowerMon* -Kategorie wird benötigt für den Zugriff auf und Nutzung des Power Monitor.

Berechtigung	Erlaubnis	Geltungsbereich
AccessPowerMonitor	Zugriff auf den Power Monitor.	Management-Station

Table 14: Berechtigungen der Kategorie PowerMon

5.1.12 Kategorie RackManager

Die *RackManager* -Kategorie umfasst die Berechtigungen für Rack-Management-Aktivitäten.

Berechtigung	Erlaubnis	Geltungsbereich
AccessRack	Rack-Gruppen überwachen (auch bekannt unter der Bezeichnung Anlagenwartung).	Alle
AccessUserGroup	Benutzerdefinierte Gruppen ansehen.	Alle
ModifyRack	Rack-Postionen bearbeiten; nicht-zugegewiesene Systeme in Racks gruppieren.	Alle
ModifyTask	Neue Tasks erzeugen.	Alle
ModifyUserGroup	Benutzerdefinierte Gruppen erzeugen und ändern.	Alle

Table 15: Berechtigungen der Kategorie RackManager

5.1.13 Kategorie RaidMgr

Die *RaidMgr* -Kategorie umfasst die Berechtigungen für den Zugriff auf den RAID Manager sowie für die RAID Konfiguration.

Berechtigung	Erlaubnis	Geltungsbereich
AccessRaidMgr	Zugriff auf den RAID Manager (Lesezugriff)	All
ModifyRaidConfig	RAID Konfiguration ändern. (Lese-/Schreib-Zugriff)	All

Table 16: Berechtigungen der Kategorie RaidMgr

5.1.14 Kategorie RemDeploy

Die *RemDeploy* -Kategorie umfasst die Berechtigungen für Installation- und Deployment-Aktivitäten.

Berechtigung	Erlaubnis	Geltungsbereich
AccessDeploymentMgr	Zugriff auf den Installation Manager.	Management-Station
AccessDeploymentMgr2	Zugriff auf Deployment Manager	Management-Station
ModifyDmNode	Server erzeugen, modifizieren und löschen; Deployment-Konfiguration exportieren und importieren.	All
ModifyDmSettings	Globale Einstellungen des Deployment Managers ändern.	All
PerformDmCreateImage	Klon-Image oder Snapshot-Image eines Servers erzeugen.	All
PerformDmDeployImage	Klon-Image oder Snapshot-Image eines Servers wiederherstellen.	All
PerformDmInstallServer	Server installieren.	All
PerformDmPowerOperations	System ein-/ausschalten.	All

Table 17: Berechtigungen der Kategorie RemDeploy

5.1.15 Kategorie ReportMgr

Die *ReportMgr* -Kategorie und die zugehörige *AccessReportMgr*-Berechtigung werden nur noch aus Kompatibilitätsgründen unterstützt und können somit ignoriert werden.

Berechtigung	Erlaubnis	Geltungsbereich
AccessReportMgr	Zugriff auf den Report Manager	CMS

Table 18: Berechtigungen der Kategorie ReportMgr

5.1.16 Kategorie SCS

Die*ModifyTrustedHosts*-Berechtigung der *SCS*-Kategorie wird für die Änderung von vertraulichen Host-Einstellungen benötigt.

Berechtigung	Erlaubnis	Geltungsbereich
ModifyTrustedHosts	Modify trusted hosts settings. **Hinweis:** Diese Berechtigung sollte nur an Benutzer vergeben werden, die bereits die *ConfigPKIt*-Berechtigung besitzen.	Managed Node

Table 19: Berechtigungen der Kategorie SCS

5.1.17 Kategorie ServerList

Die *ServerList* -Kategorie umfasst die Berechtigungen für den Zugriff auf die ServerList sowie für die Ausführung der entsprechenden Operationen.

Berechtigung	Erlaubnis	Geltungsbereich
AccessServerList	Zugriff auf die ServerList (einschließlich der impliziten Erlaubnis für den Zugriff auf den Single System View aller Systeme).	Management-Station
ModifyNode	Server und Gruppen erzeugen, ändern und löschen.	Management-Station
PerformArchiveImport	Archive importieren.	Management-Station
PerformConnectivityTest	Verbindungstest durchführen.	Management-Station
PerformDiscovery	Knoten (z.B.. Server) ermitteln und auf den Server Browser zugreifen. **Hinweis:** Diese Berechtigung kann nur einem Benutzer erteilt werden, der bereits über die Berechtigungen *PerformConnectivityTest* und *ModifyNode* verfügt.	Management-Station
PerformExploration	'explore'-Task auf Knoten (Managed Nodes) starten. **Hinweis:** Diese Berechtigung sollte nur an Benutzer vergeben werden, die bereits die *ModifyNode*-Berechtigung besitzen.	Management-Station
PerformPowerOperations	Ein-/ausschalten; System neu starten.	Management-Station

Table 20: Berechtigungen der Kategorie ServerList

5.1.18 Kategorie UpdMgr

UpdMgr -Kategorie umfasst die Berechtigungen für den Zugriff auf ServerView Download Manager / Repository Manager / Update Manager sowie für die Ausführung der entsprechenden Update-Management-Tasks.

Berechtigung	Erlaubnis	Geltungsbereich
AccessDownloadMgr	Zugriff auf den Download Manager.	Management-Station
AccessRepositoryMgr	Zugriff auf den Repository Manager.	Management-Station
AccessUpdateMgr	Zugriff auf den Update Manager.	Management-Station
DeleteJob	Einen Job löschen.	Management-Station
DeleteReleasedJob	Einen freigegebenen Job löschen.	Management-Station
ModifyUpdateConfig	Zugriff auf die Update Configuration.	Management-Station
PerformCleanUp	Daten des Update-Agent auf einem Managed Node bereinigen.	Management-Station
PerformCopyJob	Job mit Firmware/Software-Updates kopieren.	Management-Station
PerformCopyReleasedJob	Einen freigegebenen Job kopieren.	Management-Station
PerformCreateJob	Job mit Firmware/Software-Updates kopieren.	Management-Station
PerformReleaseJob	Einen Job freigeben.	Management-Station

Table 21: Berechtigungen der Kategorie UpdMgr

5.1.19 Kategorie UserMgr

Die *UserMgr* -Kategorie umfasst die Berechtigungen für den Zugriff auf den *User Management*-Wizard und dessen Verwendung für folgende Aufgaben:

– Benutzer erzeugen, ändern und löschen.
– Rollen definieren und ändern.
– Rollen an Benutzer zuweisen.

Berechtigung	Erlaubnis	Geltungsbereich
AccessUserMgr	Auf den *User Management*-Wizard zugreifen.	Management-Station
PerformUserMgt	*User Management*-Wizard für die Benutzerverwaltung mit OpenDJ verwenden.	Management-Station

Table 22: Berechtigungen der Kategorie UserMgr

5.1.20 Kategorie VIOM

Die *AccessVIOM*-Berechtigung der *VIOM* -Kategorie wird für den Zugriff auf den ServerView Virtual-IO Manager (VIOM) benötigt.

Berechtigung	Erlaubnis	Geltungsbereich
AccessVIOM	Zugriff auf VIOM.	All

Table 23: Berechtigungen der Kategorie VIOM

5.2 In OpenDJ vordefinierte Benutzer und Rollen

In OpenDJ sind die Benutzerrollen *Administrator*, *Monitor*, *Operator* und *UserAdministrator* vordefiniert und den vordefinierten Benutzern *Administrator*, *Monitor* bzw. *UserManager* permanent zugeordnet.

Die folgende Tabelle zeigt, welche Berechtigungen durch die vordefinierten Rollen erteilt werden.

Kategorie	**Berechtigung**	**Vordefinierter Benutzer / Rolle**			
		Administrator Administrator	**Operator Operator**	**Monitor Monitor**	**UserManager/ UserAdministrator**
AgentDeploy	PerformAgentDeployment	x	-	-	-
AlarmMgr	AccessAlarmMgr	x	x	x	-
	ModifyAlarmConfig	x	-	-	-
	PerformAlarmAcknowledge	x	x	-	-
	PerformMIBIntegration	x	x	-	-
ArchiveMgr	AccessArchiveMgr	x	x	-	-
	ModifyArchives	x	x	-	-
BackupMgr	ModifyBackup	x	-	-	-
	PerformBackupRestore	x	-	-	-
	PerformBackupTransfer	x	-	-	-

Table 24: Berechtigungen, die durch die vordefinierten Rollen erteilt werden

Kategorie	Berechtigung	Vordefinierter Benutzer / Rolle			
		Administrator Administrator	Operator Operator	Monitor Monitor	UserManager/ UserAdministrator
Common	AccessOnlineDiagnostics	x	x	-	-
	AccessPrimeCollect	x	x	x	-
	AccessRemoteManagement	x	x	-	-
	ConfigPKI	x	-	-	-
	ModifyCMSSettings	x	-	-	-
	ModifyPasswordTable	x	-	-	-
	PerformDownload	x	x	-	-
	PerformLocateToggle	x	x	-	-
	PerformServerErrorAck	x	x	-	-
ConfigMgr	AccessServerConfig	x	-	-	-
	ModifyPowerOnOffSettings	x	x	-	-
	ModifyServerConfig	x	-	-	-
InvMgr	AccessInvMgr	x	x	-	-
	ModifyCollections	x	-	-	-
	ModifyDiagnostics	x	x	-	-
	ModifyReports	x	-	-	-
	PerformCollections	x	x	-	-
	PerformReports	x	x	-	-
iRMC_MMB	CfgConnectionBlade	x	-	-	-
	IpmiLanOem	x	-	-	-
	IpmiLanOperator	-	x	-	-
	IpmiLanUser	-	-	x	-
	IpmiSerialOem	x	-	-	-
	IpmiSerialOperator	-	x	-	-
	IpmiSerialUser	-	-	x	-
	iRMCsettings	x	-	-	-

Table 24: Berechtigungen, die durch die vordefinierten Rollen erteilt werden

Kategorie	Berechtigung	Vordefinierter Benutzer / Rolle			
		Administrator Administrator	Operator Operator	Monitor Monitor	UserManager/ UserAdministrator
	RemoteStorage	x	-	-	-
	UserAccounts	x	-	-	-
	VideoRedirection	x	x	-	-
PerfMgr	AccessPerformanceMgr	x	x	-	-
	AccessThresholdMgr	x	x	-	-
PowerMon	AccessPowerMonitor	x	x	x	-
RackManager	AccessRack	x	x	x	-
	AccessUserGroup	x	x	x	-
	ModifyRack	x	x	-	-
	ModifyTask	x	-	-	-
	ModifyUserGroup	x	x	-	-
RaidMgr	AccessRaidMgr	x	x	x	-
	ModifyRaidConfig	x	x	-	-
RemDeploy	AccessDeploymentMgr	x	-	-	-
	AccessDeploymentMgr2	x	x	x	-
	ModifyDmNode	x	x	-	-
	ModifyDmSettings	x	-	-	-
	PerformDmCreateImage	x	x	-	-
	PerformDmDeployImage	x	-	-	-
	PerformDmInstallServer	x	-	-	-
	PerformDmPowerOperations	x	x	-	-
SCS	ModifyTrustedHosts	x	-	-	-

Table 24: Berechtigungen, die durch die vordefinierten Rollen erteilt werden

Kategorie	Berechtigung	Vordefinierter Benutzer / Rolle			
		Administrator Administrator	Operator Operator	Monitor Monitor	UserManager/ UserAdministrator
Serverliste	AccessServerList	x	x	x	-
	ModifyNode	x	x	-	-
	PerformArchiveImport	x	x	-	-
	PerformConnectivityTest	x	x	x	-
	PerformDiscovery	x	x	-	-
	PerformExploration	x	x	-	-
	PerformPowerOperations	x	x	-	-
UpdMgr	AccessDownloadMgr	x	-	-	-
	AccessRepositoryMgr	x	-	-	-
	AccessUpdateMgr	x	x	-	-
	DeleteJob	x	-	-	-
	DeleteReleasedJob	x	x	-	-
	ModifyUpdateConfig	x	-	-	-
	PerformCleanUp	x	-	-	-
	PerformCopyJob	x	-	-	-
	PerformCopyReleasedJob	x	x	-	-
	PerformCreateJob	x	-	-	-
	PerformReleaseJob	x	-	-	-
UserMgr	AccessUserMgr	-	-	-	x
	Perform UserMgt	-	-	-	x
VIOM	AccessVIOM	x	-	-	-

Table 24: Berechtigungen, die durch die vordefinierten Rollen erteilt werden

6 Audit-Logging

Mithilfe des Audit-Logging können Sie jeder in einem IT System durchgeführten Aktion den Initiator dieser Aktion zuordnen. Im Gegensatz zur Fehlerprotokollierung (Error Logging) betrachtet das Audit-Logging ausschließlich erfolgreich abgeschlossene Aktionen. Die Systemüberwachung ist nicht Ziel des Audit Logging. Audit-Logging ermöglicht autorisierten Personen die nachträgliche Auswertung von Abläufen im System.

Die im Rahmen des Audit-Logging aufgezeichneten Einträge sind für die dauerhafte Aufbewahrung bestimmt. Damit die Logging-Einträge auch aus größerem zeitlichen Abstand korrekt interpretiert werden können, muss die Beschreibung des Aufzeichnungsformats zusammen mit den Daten des Audit-Logs aufbewahrt werden.

ServerView unterstützt das komponentenspezifische Logging von Benutzeraktionen.

Derzeit ist der Centralized Authentication Service (CAS) die einzige ServerView-Komponente, die Audit-Log-Einträge erzeugt.

6.1 Lage der Audit-Log-Information im Speicher

Audit-Log-Information in Windows Systemen

In Windows Systemen werden die Audit-Log-Informationen in die Windows Ereignisanzeige geschrieben:

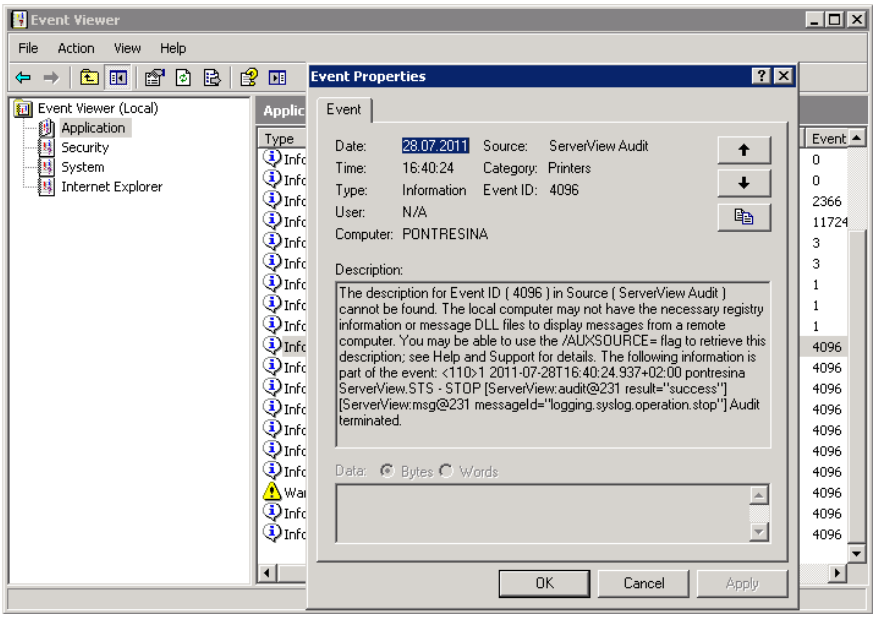

Event Viewer
File Action View Help
Event Viewer (Local)
Application
Security
System
Internet Explorer
Event Properties
Event
Date: 28.07.2011
Time: 16:40:24
Type: Information
User: N/A
Computer: PONTRESINA
Source: ServerView Audit
Category: Printers
Event ID: 4096
Description:
The description for Event ID (4096) in Source (ServerView Audit) cannot be found. The local computer may not have the necessary registry information or message DLL files to display messages from a remote computer. You may be able to use the /AUXSOURCE= flag to retrieve this description; see Help and Support for details. The following information is part of the event: <110>1 2011-07-28T16:40:24.937+02:00 pontresina ServerView.STS - STOP [ServerView:audit@231 result="success"] [ServerView:msg@231 messageId="logging.syslog.operation.stop"] Audit terminated.
Data: Bytes Words
OK
Cancel
Apply

Bild 33: Der ServerView Audit-Log ist Bestandteil der Windows Ereignisanzeige.

Audit-Log-Information in Linux Systemen

In Linux Systemen werden die Audit-Log-Informationen in die UTF-8-codierte Datei *audit.log* geschrieben, die im Verzeichnis */var/log/fujitsu/ServerViewSuite/jboss* liegt. Die Datei *audit.log* wird täglich neu erzeugt. Die Vorgängerdatei der aktuellen *audit.log* -Datei wird umbenannt in *audit.log.<YYYY-MM-DD>.log*, wobei *<YYYY-MM-DD>* jeweils das Datum des Vortags angibt.

6.2 Einträge des Audit-Logs

Jede Zeile der Audit-Log-Datei repräsentiert einen Eintrag im Audit-Log. Die Struktur der Einträge in der Audit-Log-Datei basiert auf dem RFC 5424 (Syslog protocol).

Jeder Logging-Eintrag besteht aus einem Header, auf den die strukturierten Daten folgen:

– Der Header enthält eine Liste der Felder, die in jedem Eintrag vorhanden sind.

– Die strukturierten Daten (STRUCTURED-DATA in RFC 5424) liefern eine detaillierte Beschreibung der protokollierten Daten.

– Eine detaillierte Beschreibung der Syntax-Elemente finden Sie in RFC 5424.

– Zu Beispielen zu Logging-Einträgen siehe Abschnitt "Beispiele: Einträge in der Audit-Log-Datei" auf Seite 146).

6.2.1 Typen von Audit-Log-Einträgen

Drei Typen von Audit-Log-Einträgen sind zu unterscheiden:

- `INIT`-Eintrag

  Der `INIT`-Eintrag ist immer der erste Eintrag der Audit-Log-Datei und wie folgt strukturiert:

  – Header
  – `ServerView:audit@231`-Element
  – `origin`-Element
  – `ServerView:env@231`-Element
  – Freitext, der auf die strukturierten Daten folgt.

- `<operation>`-Eintrag

  Ein `<operation>`-Eintrag bezieht sich auf eine Operation `<operation>`, die in der durch `<COMP_Name>` spezifizierten Komponente ausgeführt wurde.

  Ein `<operation>`-Eintrag ist wie folgt strukturiert:

  – Header
  – `ServerView.<COMP_Name>:audit@231`-Element
  – Freitext, der auf die strukturierten Daten folgt.

- `STOP`-Eintrag

  Der `STOP`-Eintrag ist in der Regel der letzte Eintrag in der Audit-Log-Datei und wie folgt strukturiert:

  – Header
  – `ServerView:audit@231`-Element
  – Freitext, der auf die strukturierten Daten folgt.

  Falls die protokollierte Komponente fehlerhaft beendet wurde, ist der `STOP`-Eintrag möglicherweise nicht vorhanden.

In den folgenden Abschnitten sind die oben erwähnten Komponenten (Header, Elemente) der Audit-Log-Einträge detailliert beschrieben.

6.2.2 Header eines Audit-Log-Eintrags

Der Header besteht aus den folgenden Feldern, von denen jeweils zwei durch ein Leerzeichen getrennt sind.

Feldinhalt	Beschreibung:
<108>1 / <110>1	Diese Felder haben gemäß RFC 5424 folgende Bedeutung: <108> 1 resultiert aus <(**13** * 8) + **4**> **1** und spezifiziert im Einzelnen: Syslog facility: **13** (log audit) Syslog severity: **4** (warning) Syslog protocol: version **1** <108> 1 resultiert aus <(**13** * 8) + **4**> **1** und spezifiziert im Einzelnen: Syslog facility: **13** (log audit) Syslog severity: **6** (informational) Syslog protocol: version **1**
Timestamp	Zeitstempel gemäß dem in RFC 3339 spezifizierten Format.
Computer name	Rechnername
ServerView component	Name der ServerView-Komponente. Zurzeit ist `ServerView.CAS` die einzige ServerView-Komponente, die Logging-Einträge schreibt.
-	Ist in jeder Zeile konstant. Die Prozess ID wird nicht protokolliert (entsprechend RFC 5424).
MsgId	Name der Operation in abdruckbarem Format. Falls es sich um Einträge von Servern der Version 3 handelt, sind dies Operationen der ServerView-Komponenten.

Tabelle 25: Header eines Audit-Log-Eintrags

Beispiel

<110>1	2011-07-07T09:42:03,113+02:00	compA1	ServerView CAS	-	LOGIN

6.2.3 Strukturierte Daten eines Audit-Log-Eintrags

Auf den Header eines Audit-Log-Eintrags folgen die strukturierten Daten, die das Ereignis beschreiben. Die strukturierten Daten sind vom Header durch ein Leerzeichen getrennt.

Die strukturierten Daten setzen sich zusammen aus einer Liste von Elementen (SD-ELEMENT in RFC 5424), von denen jedes in eckige Klammern eingeschlossen ist ([ ]).

Innerhalb der eckigen Klammern beginnt jedes Element mit einen Elementnamen (SD-NAME in RFC 5424), gefolgt von einer Liste von Parametern, die als "Schlüssel/ Wert"-Paare formatiert sind (SD-PARAM in RFC 5424). Jeder Wert ist in doppelte Hochkommata (") eingeschlossen.

Die Reihenfolge der Elemente ist nicht festgelegt. Welche Elemente und Werte vorhanden sind, hängt vom jeweiligen Ereignis ab. Die Elemente und Werte sind weiter unten detailliert beschrieben.

Die Audit-Log-Einträge enthalten die nachfolgend beschriebenen Elemente, wobei `COMP_NAME` den Namen der zugehörigen Komponente bezeichnet.

Das Element mit Namen `ServerView.COMP_NAME:audit@231` ist in jedem Eintrag enthalten. Alle anderen Elemente sind optional.

6.2.3.1 origin-Element

Das *origin*-Element ist in Einträgen mit der MsgId `INIT` enthalten. Der Elementname *origin* und die Bedeutung seiner Parameter sind bei der Internet Assigned Numbers Authority (IANA) for RFC 5424 registriert und haben demzufolge kein Suffix `@231`. Das *origin*-Element enthält Informationen darüber, welches Produkt welches Lieferanten den Logging-Eintrag erzeugt hat.

Parameter	Bedeutung
Software	Produktname (immer ServerView) und Komponentenname (z.B. CAS).
swVersion	Version der ServerView-Komponente zum Zeitpunkt, als der Audit-Log-Eintrag erzeugt wurde.
enterpriseId	Private Enterprise Number, die für eine Firma bei IANA registriert ist. Die Private Enterprise Number für Fujitsu Technology Solutions lautet 231.

Tabelle 26: Audit-Log-Eintrag - origin Element

6.2.3.2 ServerView:env@231-Element

Das *ServerView:env@23* -Element ist nur in Logging-Einträgen mit Msgid `INIT` enthalten. Es enthält Informationen über die Laufzeitumgebung (Runtime Environment).

Parameter	Bedeutung
javaHome	Java-Installationsverzeichnis
javaVendor	Anbieter des Java Runtime Environment (JRE)
jbossUserDir	Aktuelles Arbeitsverzeichnis des JBoss-Nutzers
jbossUserHome	Home-Verzeichnis des JBoss-Nutzers
jbossUserName	Kennung des JBoss-Nutzers
osName	Name des Betriebssystems
osVersion	Version des Betriebssystems

Tabelle 27: Audit-Log-Eintrag - ServerView:env@231-Element

6.2.3.3 ServerView:audit@231-Element

Der *ServerView:audit@231*-Eintrag ist Bestandteil jedes Audit-Log-Eintrags. "231" ist die Private Enterprise Number für Fujitsu Technology Solutions, die bei Internet Assigned Numbers Authority (IANA) registriert ist. Somit identifiziert das suffix "@231" das Element als reserviertes Element für Fujitsu Technology Solutions entsprechend RFC 5424.

Parameter	Bedeutung
Ergebnis	Gibt an, ob die Operation erfolgreich ausgeführt wurde. Mögliche Werte sind: "success": Die Operation wurde ausgeführt. "failure": Die Operation schlug fehl.

Tabelle 28: Audit-Log-Eintrag - ServerView:audit@231-Element

6.2.3.4 ServerView[.<COMP_NAME>]:msg@231-Element

Der *ServerView[.<COMP_NAME>]:msg@231-Element*-Eintrag ist Bestandteil jedes Audit-Log-Eintrags. Der Eintrag enthält die ID, die sich auf die Meldung bezieht, die die aktuelle Operation erklärt.

<COMP_NAME> bezeichnet die ServerView-Komponente, die den Audit-Log-Eintrag liefert. Einige Meldungen beziehen sich auf alle ServerView-Komponenten. In diesen Fällen fehlt der Namensbestandteil .*<COMP_NAME>*.

"231" ist die Private Enterprise Number für Fujitsu Technology Solutions, die bei Internet Assigned Numbers Authority (IANA) registriert ist. Somit identifiziert das suffix "@231" das Element als reserviertes Element für Fujitsu Technology Solutions entsprechend RFC 5424.

Parameter	Bedeutung
messageId	Meldungs-ID, die sich auf die Meldung bezieht, die die aktuelle Operation erklärt.

Tabelle 29: Audit-Log-Eintrag - ServerView[.<COMP_NAME>]:msg@231-Element

6.2.3.5 ServerView[.<COMP_NAME>]:<operation>@231-Element

Dieses Element ist spezifisch für ServerView-Komponenten und in jedem Audit-Log-Eintrag mit der Msgid *<operation>* einmal enthalten. Das Element beschreibt die Details eines Requests zur Ausführung einer Operation.

Welche Parameter genau in einem Element enthalten sind, hängt von der jeweiligen Operation und ihrem Ergebnis ab. Derzeit sind der Centralized Authentication Service (`COMP_NAME = CAS`) und der Security Token Service (`COMP_NAME = STS`) die einzigen ServerView-Komponenten, die Audit-Logging unterstützen .

Nachfolgend ist die Struktur der von den ServerView-Komponenten CAS und STS erstellten Audit-Log-Einträge beschrieben.

ServerView-Komponente CAS

Der folgende Audit-Log-Eintrag wird immer dann erzeugt, wenn ein Benutzer versucht, sich bei einer ServerView-Sitzung anzumelden.

```
MSG-ID = LOGIN
SD-ID = ServerView.CAS:login@231
```

Parameter	Bedeutung
address	IP-Adresse des Zielsystems
user	Benutzerkennung, die beim Login angegeben wurde.
tgt	CAS Ticket Granting Ticket, das beim Login erzeugt wurde.

Tabelle 30: Audit-Log-Eintrag - Parameter von ServerView.CAS:login@231

Der folgende Audit-Log-Eintrag wird immer dann erzeugt, wenn ein Benutzer bei einer ServerView-Sitzung abmeldet.

```
MSG-ID = LOGOUT
SD-ID = ServerView.CAS:logout@231
```

Parameter	Bedeutung
address	IP-Adresse des Zielsystems
user	Benutzerkennung, die beim Logout angegeben wurde.
tgt	CAS Ticket Granting Ticket, das beim Login erzeugt wurde.

Tabelle 31: Audit-Log-Eintrag - Parameter von ServerView.CAS:login@231

ServerView-Komponente STS

Der folgende Audit-Log-Eintrag wird immer dann erzeugt, wenn ein STS-Client ein binäres Sicherheits-Token anfordert, das ein CAS Ticket Granting Ticket (TGT) enthält.

```
MSG-ID = RST_ISSUE_TGT
SD-ID = ServerView.STS:rstIssueTgt@231
```

Parameter	Bedeutung
address	IP-Adresse des Zielsystems
user	Benutzerkennung, die mit dem Username-Token in der RST "issue TGT" Anforderung angegeben wurde.
tgt	CAS Ticket Granting Ticket, das beim Login erzeugt wurde.

Tabelle 32: Audit-Log-Eintrag - Parameter von ServerView.STS:rstIssueTgt@231

Der folgende Audit-Log-Eintrag wird immer dann erzeugt, wenn ein STS-Client ein binäres Sicherheits-Token anfordert, das ein CAS Ticket Granting Ticket (ST) enthält.

```
MSG-ID = RST_ISSUE_ST
SD-ID = ServerView.STS:rstIssueSt@231
```

Parameter	Bedeutung
address	IP-Adresse des Zielsystems
tgt	CAS Ticket Granting Ticket, das mit dem binären Sicherheits-Token im RST Request angegeben wurde.
st	CAS Service Ticket, das das durch den RST "issue ST" Request erzeugt wurde.

Tabelle 33: Audit-Log-Eintrag - Parameter von ServerView.STS:rstIssueSt@231

Der folgende Audit-Log-Eintrag wird immer dann erzeugt, wenn ein STS-Client ein binäres Sicherheits-Token anfordert, das ein CAS Ticket Granting Ticket (ST) enthält.

```
MSG-ID = VALIDATE
SD-ID = ServerView.STS:validate@231
```

Parameter	Bedeutung
address	IP-Adresse des Zielsystems
st	CAS Service Ticket, das das durch den RST "issue ST" Request erzeugt wurde.
user	Benutzerkennung, die mit dem Username-Token in der RST "issue TGT" Anforderung angegeben wurde.

Tabelle 34: Audit-Log-Eintrag - Parameter von ServerView.STS:validate@231

6.2.4 Beispiele: Einträge in der Audit-Log-Datei

Die folgenden Beispiele zeigen die Audit-Log-Einträge des Centralized Authentication Service (CAS) von ServerView. Zur besseren Lesbarkeit wurden zusätzliche Zeilen eingefügt.

INIT-Eintrag

Der folgende `INIT`-Eintrag enthält die Elemente `origin`, `ServerView:audit@231` und `ServerView.CAS:env@231`sowie Freitext im Anschluss an die strukturierten Daten:

```
<110>1 2011-07-20T08:33:16,265+02:00 pontresina
ServerView CAS Suite - INIT
[ServerView:audit@231 result="success"]
[ServerView:env@231 javaHome="C:\\Program Files\\Java\\jre7"
javaVendor="Sun Microsystems Inc." javaVersion="1.6.0_26"
jbossUserDir="C:\\Program Files\\Fujitsu\\ServerView
Suite\\jboss\\bin" jbossUserHome="D:\\Profiles\\jbossrun"
jbossUserName="jbossrun" osName="Windows XP" osVersion="5,1"]
[ServerView:msg@231 messageId="logging.syslog.operation.init"]
[origin enterpriseId="231" software="ServerView.CAS" swVersion=
"SVCOM_V1.50/3.3,2"] Audit started
```

LOGIN-Entry (fehlgeschlagenes Login)

Der folgende `LOGIN`-Eintrag enthält das Element `ServerView:audit@231` sowie Freitext im Anschluss an die strukturierten Daten. Dieser Eintrag stellt einen "Warning"-Eintrag dar, der durch ein fehlgeschlagenes Login verursacht wurde.

```
<108>1 2011-07-20T08:38:52,234+02:00 pontresina
ServerView.CAS - LOGIN
[ServerView.CAS:login@231 address="172.25.88.121"]
[ServerView.CAS:msg@231 messageId=
"error.authentication.credentials.bad"]
[ServerView:audit@231 result="failure"] The credentials you
provided cannot be determined to be authentic.
```

LOGIN-Eintrag (erfolgreiches Login)

Der folgende, von einem erfolgreichen Login verursachte `LOGIN`-Eintrag enthält das Element `ServerView:audit@231` sowie Freitext im Anschluss an die strukturierten Daten.

```
<110>1 2011-07-20T08:38:32,406+02:00 pontresina
ServerView.CAS - LOGIN
[ServerView.CAS:login@231 address="172.25.88.121" tgt=
"TGT-1-VSOg93zTt2dZQ1WX1texuXNEmJKvw21HelXqXIScvMKVi7XOBY-cas"
user="administrator"]
[ServerView.CAS:msg@231 messageId="screen.success.header"]
[ServerView:audit@231 result="success"]
Log In Successful
```

LOGOUT-Eintrag

Der folgende `LOGOUT`-Eintrag enthält das Element `ServerView:audit@231` sowie Freitext im Anschluss an die strukturierten Daten.

```
<110>1 2011-07-20T08:38:35,156+02:00 pontresina
ServerView.CAS - LOGOUT
[ServerView.CAS:login@231 address="172.25.88.121" tgt=
"TGT-1-VSOg93zTt2dZQ1WX1texuXNEmJKvw21HelXqXIScvMKVi7XOBY-cas"
user="administrator"]
[ServerView.CAS:msg@231 messageId="screen.logout.header"]
[ServerView:audit@231 result="success"]
Logout successful
```

STOP-Eintrag

Der folgende `LOGIN`-Eintrag enthält das Element `ServerView:audit@231` sowie Freitext im Anschluss an die strukturierten Daten.

```
<110>1 2011-07-20T08:39:07,468+02:00 pontresina
ServerView.CAS - STOP
[ServerView:audit@231 result="success"]
[ServerView:msg@231 messageId"logging.syslog.operation.stop"]
Audit terminated
```

7 Anhang 1 - Globale iRMC S2/S3-Benutzerverwaltung via Verzeichnisdienst

Die Benutzerverwaltung für den iRMC S2/S3 verwendet zwei verschiedene Arten von Benutzerkennungen:

– **Lokale Benutzerkennungen** sind lokal im nicht-flüchtigen Speicher des iRMC S2/S3 hinterlegt und werden über die Benutzerschnittstellen des iRMC S2/S3 verwaltet.

– **Globale Benutzerkennungen** sind in der zentralen Datenhaltung eines Verzeichnisdienstes (Directory Service) hinterlegt und werden über die Schnittstellen dieses Verzeichnisdienstes verwaltet.

  Für die globale iRMC S2/S3-Benutzerverwaltung werden zurzeit folgende Verzeichnisdienste unterstützt:

  – Microsoft® Active Directory
  – Novell® eDirectory
  – OpenLDAP
  – ForgeRock OpenDJ (Bei ServerView wird dieser Verzeichnisdienst im "embedded" Modus unter JBoss ausgeführt.)

Das vorliegende Kapitel informiert über folgende Themen:

– Konzept der Benutzerverwaltung für den iRMC S2/S3
– Benutzerberechtigungen
– globale Benutzerverwaltung mithilfe der einzelnen Verzeichnisdienste

Einzelheiten zur lokalen Benutzerverwaltung des iRMC S2/S3 finden Sie im Handbuch „iRMC S2/S3 - integrated Remote Management Controller“.

In SeverView’s OpenDJ, ausgeführt im "embedded" Modus unter JBoss wird die Funktion *E-Mail-Einstellungen* des iRMC S2/S3 nicht unterstützt.

7.1 Konzept der Benutzerverwaltung für den iRMC S2/S3

Die Benutzerverwaltung für den iRMC S2/S3 unterstützt die parallele Verwaltung lokaler und globaler Benutzerkennungen.

Bei der Validierung der Authentisierungsdaten (Benutzername, Passwort), die ein Benutzer beim Login an einer der iRMC S2/S3-Schnittstellen eingibt, verfährt der iRMC S2/S3 gemäß dem folgenden Ablauf (siehe auch Bild 34 auf Seite 151):

1. Der iRMC S2/S3 gleicht den Benutzernamen und das Passwort mit den lokal gespeicherten Benutzerkennungen ab:
   - Bei erfolgreicher Authentifizierung des Benutzers durch den iRMC S2/S3 (Benutzername und Passwort sind gültig) darf sich der Benutzer einloggen.
   - Andernfalls setzt der iRMC S2/S3 die Prüfung mit Schritt 2. fort.
2. Der iRMC S2/S3 authentisiert sich beim Verzeichnisdienst via LDAP mit Benutzernamen und Passwort, ermittelt per LDAP-Anfrage die Benutzerrechte und prüft, ob der Benutzer damit am iRMC S2/S3 arbeiten darf.

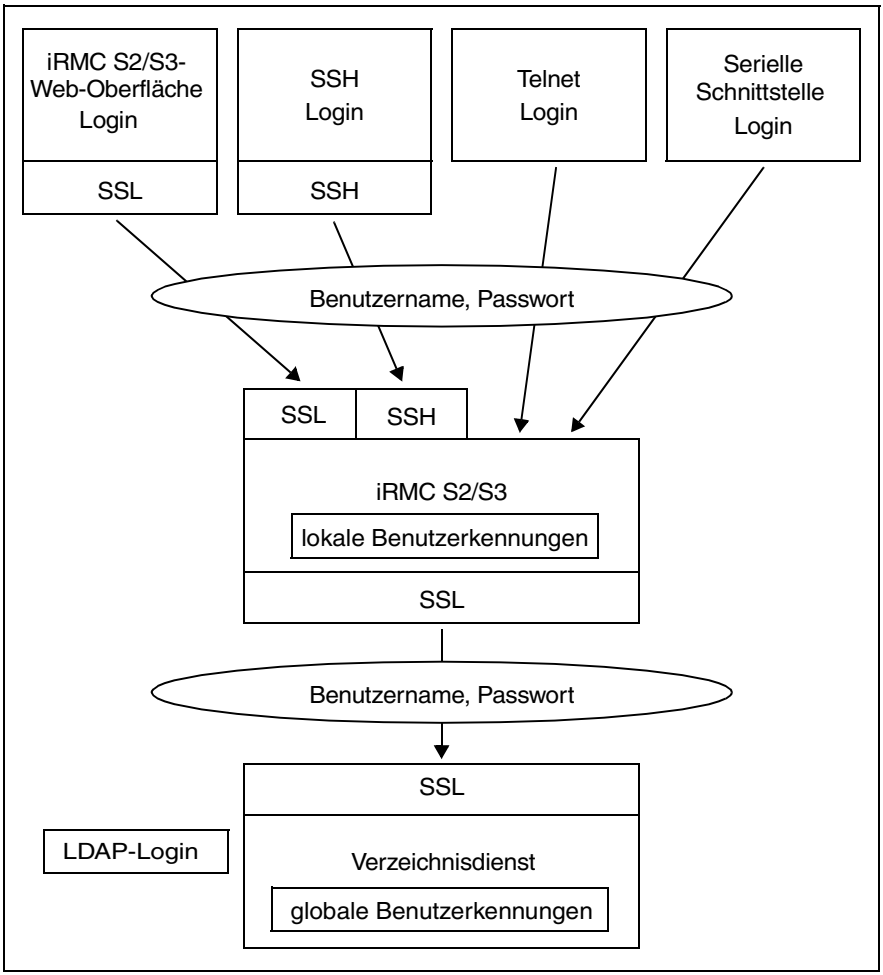


Bild 34: Login-Authentifizierung durch den iRMC S2/S3

Die Nutzung von SSL für die LDAP-Verbindung zwischen dem iRMC S2/S3 und dem Verzeichnisdienst ist optional, wird jedoch empfohlen. Eine SSL-gesicherte LDAP-Verbindung zwischen iRMC S2/S3 und Verzeichnisdienst garantiert den sicheren Austausch der Daten, insbesondere auch von Benutzernamen und Passwort.

SSL-Login über die iRMC S2/S3-Web-Oberfläche ist nur dann erforderlich, wenn LDAP aktiviert ist (siehe Handbuch "iRMC S2/S3 integrated Remote Management Controller").

7.2 Globale Benutzerverwaltung für den iRMC S2/S3

Die globalen Benutzerkennungen für den iRMC S2/S3 werden zentral für alle Plattformen mithilfe eines LDAP-Verzeichnisdienstes verwaltet.

Für die iRMC S2/S3-Benutzerverwaltung werden zurzeit folgende Verzeichnisdienste unterstützt:

- Microsoft® Active Directory
- Novell® eDirectory
- OpenLDAP
- Open DS / ForgeRock's OpenDJ

Dieser Abschnitt informiert über folgende Themen:

- Überblick über die globale Benutzerverwaltung für den iRMC S2/S3
- Konzept der globalen Benutzerverwaltung für den iRMC S2/S3 mithilfe eines LDAP-Verzeichnisdienstes
- Globale iRMC S2/S3-Benutzerverwaltung im Verzeichnisdienst konfigurieren (iRMC S2/S3-spezifische Berechtigungsstrukturen im Verzeichnisdienst generieren).
- Globale iRMC S2/S3-Benutzerverwaltung via Microsoft Active Directory
- Globale iRMC S2/S3-Benutzerverwaltung via Novell eDirectory
- Globale iRMC S2/S3-Benutzerverwaltung via OpenLDAP/ OpenDS / OpenDJ

Neben den in diesem Abschnitt beschriebenen Maßnahmen, die Sie auf Seiten des Verzeichnisdienstes durchführen, erfordert die globale Benutzerverwaltung außerdem die Konfiguration der lokalen LDAP-Einstellungen am iRMC S2/S3.

Die lokalen LDAP-Einstellungen konfigurieren Sie wahlweise (siehe Handbuch "iRMC S2/S3 - integrated Remote Management Controller"):

- an der iRMC S2/S3-Web-Oberfläche,
- mithilfe des Server Configuration Managers.

Die Konfiguration der Einstellungen für die globale iRMC S2/S3-Benutzerverwaltung erfordert detaillierte Kenntnisse des verwendeten Verzeichnisdienstes. Nur Personen mit den entsprechenden Kenntnissen sollten die Konfiguration durchführen.

7.2.1 Überblick

Die globalen Benutzerkennungen für den iRMC S2/S3 (wie auch für den iRMC) werden zentral und Plattform-übergreifend im Verzeichnis (Directory) eines Verzeichnisdienstes abgelegt. Auf diese Weise lassen sich die Benutzerkennungen auf einem zentralen Server verwalten und können somit von allen iRMC und iRMC S2/S3 verwendet werden, die mit diesem Server im Netz verbunden sind.

Der Einsatz eines Verzeichnisdienstes für den iRMC S2/S3 ermöglicht es darüber hinaus, für das Anmelden an den iRMC S2/S3 dieselben Benutzerkennungen zu verwenden wie für das Anmelden am Betriebssystem der verwalteten Server.

Für die folgenden iRMC S2/S3-Funktionen wird zurzeit die globale Benutzerverwaltung nicht unterstützt:

- Login via IPMI-over-LAN
- Text-Konsolen-Umleitung via SOL

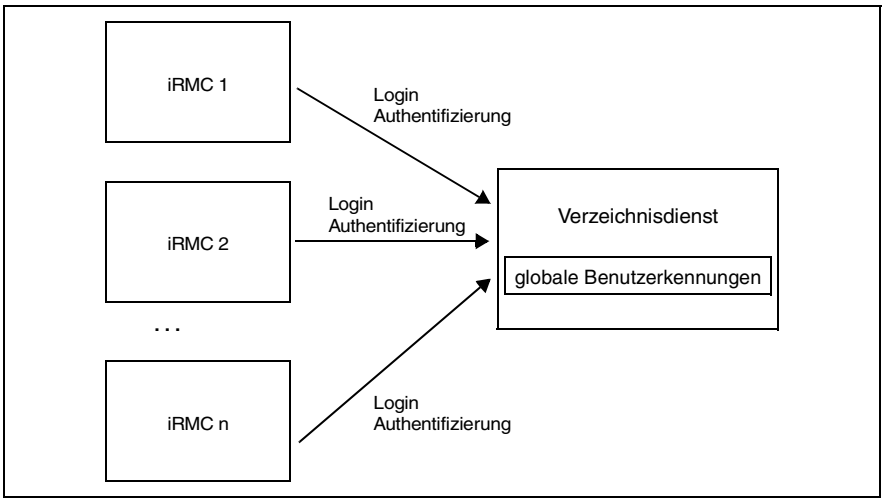


Bild 35: Gemeinsame Nutzung der globalen Benutzerkennungen durch mehrere iRMC S2/S3

Die Kommunikation zwischen den einzelnen iRMC S2/S3 und dem zentralen Verzeichnisdienst wird über das TCP/IP-Protokoll LDAP (**L**ightweight **D**irectory **A**ccess **P**rotocol) abgewickelt. LDAP ermöglicht den Zugriff auf die gängigsten zur Benutzerverwaltung geeigneten Verzeichnisdienste. Die Kommunikation über LDAP kann optional durch SSL abgesichert werden.

7.2.2 iRMC S2/S3-Benutzerverwaltung mithilfe eines LDAP-Verzeichnisdienstes (Konzept)

Das im Folgenden erläuterte Konzept einer Verzeichnisdienst-gestützten, globalen iRMC S2/S3-Benutzerverwaltung gilt gleichermaßen für die Verzeichnisdienste Microsoft Active Directory, Novell eDirectory, OpenLDAP und OpenDS / OpenDJ. Die Abbildungen zeigen exemplarisch die Konsole *Active Directory-Benutzer und -Computer* der Benutzeroberfläche von Microsoft Active Directory.

Die folgenden Zeichen sind in LDAP als Meta-Zeichen für Such-Strings reserviert: *, \, &, (,), |, !, =, <, >, ~, :

Verwenden Sie diese Zeichen deshalb nicht als Bestandteil von Relative Distinguished Names (RDN).

7.2.2.1 Globale iRMC S2/S3-Benutzerverwaltung über Berechtigungsgruppen und Rollen

Die globale iRMC S2/S3-Benutzerverwaltung mithilfe eines LDAP-Verzeichnisservers (LDAP Directory Server) erfordert keine Erweiterung des Standard-Schemas des Verzeichnisservers. Vielmehr werden sämtliche für den iRMC S2/S3 relevanten Informationen einschließlich der Benutzerberechtigungen (Privilegien) über zusätzliche LDAP-Gruppen und Organisationseinheiten (Organizational Units, OU) bereitgestellt, die in einer separaten OU innerhalb einer Domäne des LDAP-Verzeichnisservers in separaten OUs zusammengefasst sind (siehe Bild 37 auf Seite 157).

iRMC S2/S3-Benutzer erhalten ihre Privilegien über die Zuweisung einer in der Organizational Unit (OU) *SVS* deklarierten Rolle (Benutzerrolle).

Rechtevergabe über Benutzerrollen (kurz: Rollen, Role)

Die globalen Benutzerverwaltung am iRMC S2/S3 (Firmware-Version 3.77 oder höher) regelt die Rechtevergabe über Benutzerrollen. Dabei definiert jede Rolle ein spezifisches, aufgabenorientiertes Berechtigungsprofil für Tätigkeiten am iRMC S2/S3.

Jedem Benutzer können mehrere Rollen zugewiesen werden, sodass sich die Rechte dieses Benutzers aus der Gesamtheit der Rechte aller zugewiesenen Rollen ableiten.

Bild 36 skizziert das Konzept der rollenbasierten Vergabe von Benutzerberechtingungen mit den Rollen *Administrator*, *Maintenance*, *Observer* und *UserKVM*.

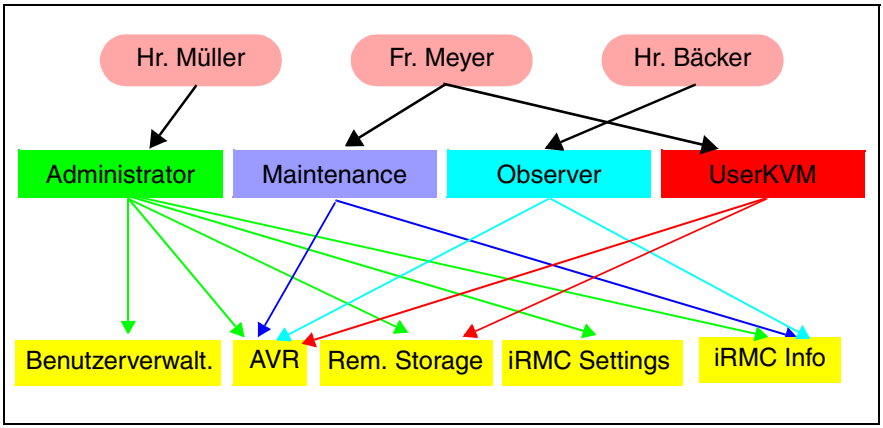


Bild 36: Rollenbasierten Vergabe von Benutzerberechtigungen

Das Konzept der Benutzerrollen bietet u.a folgende wesentlichen Vorteile:

– Die einzelnen Berechtigungen müssen nicht jedem Benutzer oder jeder Benutzergruppe separat zugewiesen werden, sondern nur der Benutzerrolle.

– Wenn sich die Berechtigungsstruktur ändert, müssen nur die Rechte der Benutzerrolle angepasst werden.

7.2.2.2 Organizational Unit (OU) SVS

Die Firmware des iRMC S2 ab Firmware-Version 3,77A und des iRMC S3 unterstützen LDAP v2-Strukturen, die in der OU *SVS* abgelegt sind. LDAP v2-Strukturen sind für künftige funktionale Erweiterungen ausgelegt.

Eine zusätzliche OU (*iRMCgroups*), die aus Kompatibilitätsgründen unterstützt wird, ermöglicht Ihnen die globale Benutzerverwaltung in Verbindung mit iRMC S2s mit einer Firmware-Version < 3,77 mit iRMCs.

Näheres hierzu finden Sie in den folgenden Handbüchern:

- "iRMC S2/S3 - integrated Remote Management Controller", Ausgabe Mai 2011 und frühere Ausgaben.
- "iRMC - integrated Remote Management Controller"

SVS enthält die OUs *Declarations*, *Departments* und *User Settings*:

- *Declarations* enthält eine Liste der definierten Rollen sowie die Liste der vordefinierten iRMC S2/S3-Benutzerberechtigungen (siehe Handbuch "iRMC S2/S3 - integrated Remote Management Controller").
- *Departments* enthält die Gruppen für die Benutzerprivilegien.
- *User Settings* enthält Benutzer(gruppen)-spezifische Angaben, wie z.B. das Mail-Format (für die E-Mail-Benachrichtigung) und die Gruppen für die Benutzershells.

Bei Microsoft Active Directory z.B. können die Einträge für die iRMC S2/S3-Benutzer in der Standard OU *Users* liegen. Im Gegensatz zu den Standardbenutzern sind iRMC S2/S3-Benutzer jedoch zusätzlich Mitglied in einer oder mehreren Gruppen der OU *SVS*.

Wichtiger Hinweis:

Die Abwicklung sowohl der ServerView- als auch des iRMC S2/S3-Benutzerverwaltung innerhalb derselben Organizational Unit (OU) SVS setzt voraus, dass der iRMC S2/S3 als Element des Departments DEFAULT konfiguriert ist.

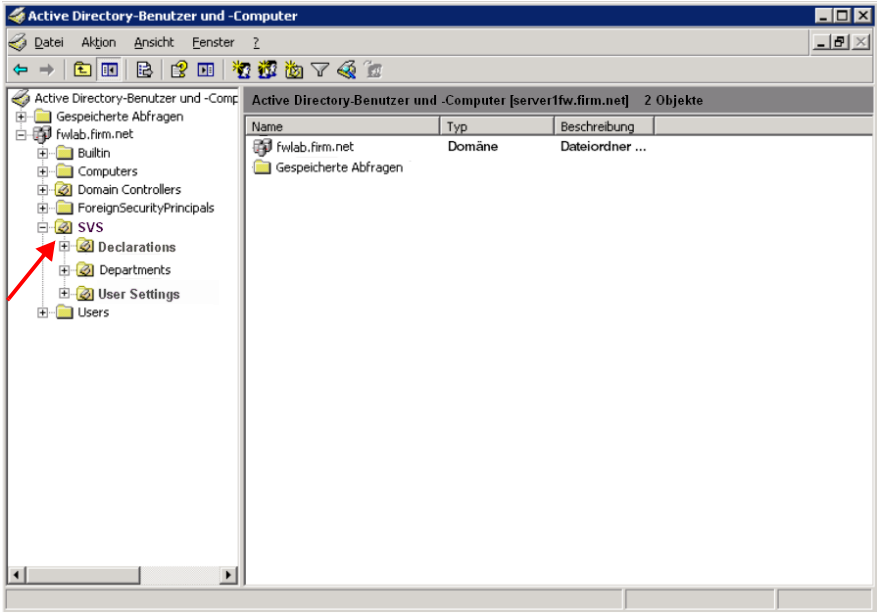


Bild 37: OU SVS in der Domäne fwlab.firm.net

Die Benutzereinträge für den iRMC S2/S3 können ab der Firmware-Version 3.6x an beliebigen Stellen unterhalb der Basis-Domäne liegen. Ebenso können Berechtigungsgruppen an beliebigen Stellen innerhalb der Basisdomäne liegen.

7.2.2.3 Server-übergreifende globale Benutzerberechtigungen

In größeren Unternehmen sind die via iRMC S2/S3 verwalteten Server in der Regel verschiedenen Abteilungen zugeordnet. Außerdem werden die Administrator-Berechtigungen für die verwalteten Server ebenfalls oft abteilungsspezifisch vergeben.

Wichtiger Hinweis:

Die Abwicklung sowohl der ServerView- als auch der iRMC S2/S3-Benutzerverwaltung innerhalb derselben Organizational Unit (OU) SVS setzt voraus, dass der iRMC S2/S3 als Element des Departments DEFAULT konfiguriert ist.

Abteilungen sind in der OU „Departments“ zusammengefasst

Die OU *Departments* fasst die via iRMC S2/S3 verwalteten Server zu verschiedenen Gruppen zusammen. Diese entsprechen den Abteilungen, in denen jeweils dieselben Benutzerkennungen und -berechtigungen gelten. In Bild 38 auf Seite 159 z.B. sind dies die Abteilungen *DeptX*, *DeptY* und *Others*.

Der Eintrag *Others* ist optional, wird aber empfohlen. *Others* ist eine vordefinierte Abteilungsbezeichnung, unter der diejenigen Server zusammengefasst sind, die keiner anderen Abteilung angehören. Die Anzahl der unter *Departments* aufgelisteten Abteilungen (OUs) unterliegt keinen Einschränkungen.

Bei der Konfiguration des Verzeichnisdienstes am iRMC S2/S3 über die iRMC S2/S3-Web-Oberfläche oder über den Server Configuration Manager spezifizieren Sie den Namen der Abteilung, welcher der verwaltete Server mit dem betreffenden iRMC S2/S3 angehört. Existiert im LDAP-Verzeichnis keine Abteilung dieses Namens, dann werden die Berechtigungen der Abteilung *Others* verwendet.

Bild 38 auf Seite 159 zeigt anhand von *Active Directory-Benutzer und -Computer* ein Beispiel für eine solche Organisationsstruktur.

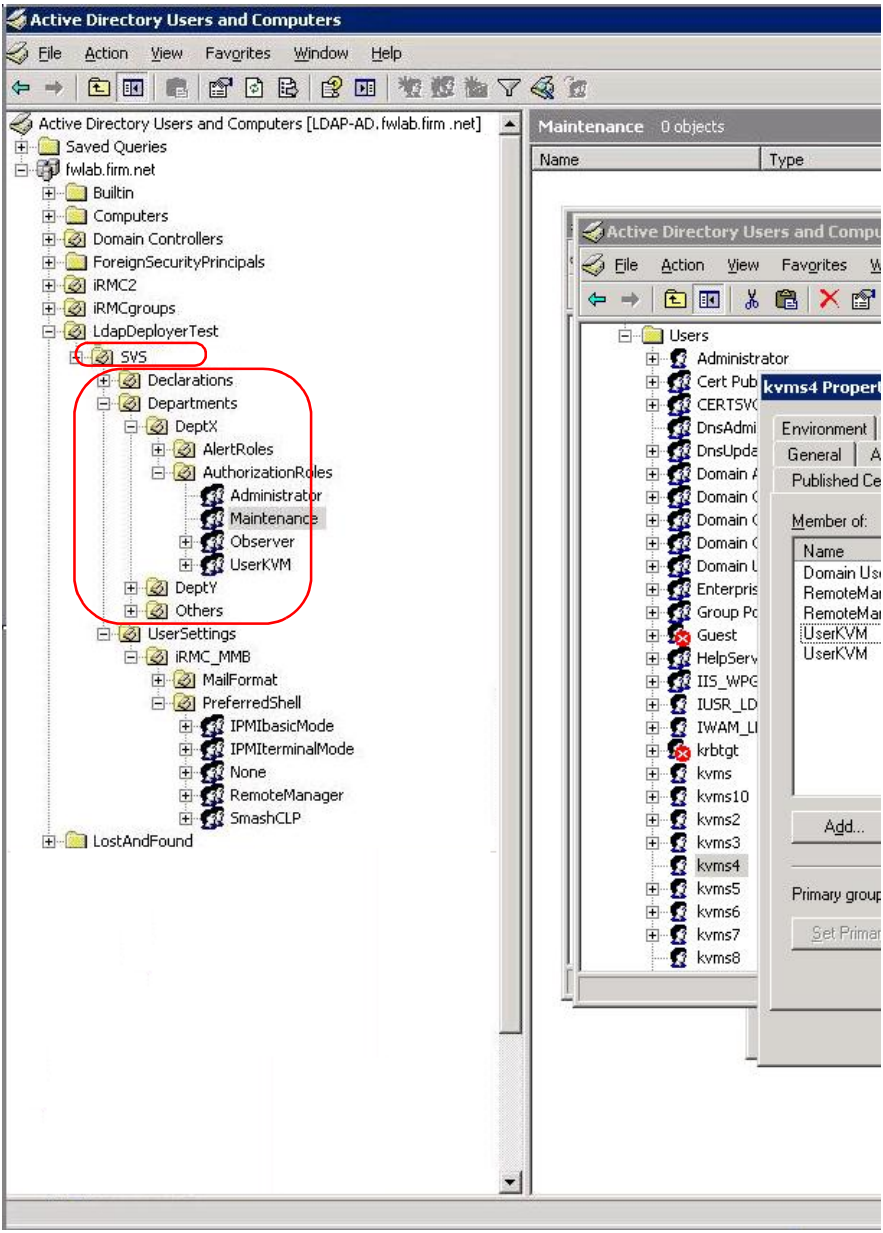


Bild 38: Organistionsstruktur der Domäne fwlab.firm.net

7.2.2.4 SVS: Berechtigungsprofile werden über Rollen definiert

Direkt unterhalb jeder Abteilung sind die gewünschten zugehörigen Benutzerrollen (Authorization Roles) aufgeführt (Bild 38 auf Seite 159). Alle hier aufgeführten Rollen müssen in der OU *Declarations* definiert sein. Ansonsten gibt es hinsichtlich Anzahl der Roles keine Einschränkungen. Die Namen der Rollen sind unter Beachtung einiger syntaktischer Vorgaben des verwendeten Verzeichnisdienstes frei wählbar. Jede Authorization Role definiert ein spezifisches, aufgabenorientiertes Berechtigungsprofil für Tätigkeiten am iRMC S2/S3.

Neben den Authorization Roles sind auch die Alert Roles aufgeführt. Jede Alert Role definiert ein spezifisches Benachrichtigungsprofil für die E-Mail-Benachrichtigung (siehe Abschnitt "E-Mail-Benachrichtigung an globale iRMC S2/S3-Benutzer konfigurieren" auf Seite 219).

Benutzerrollen anzeigen

Wenn Sie im Strukturbaum von *Active Directory-Benutzer und -Computer* (siehe Bild 39) unter *SVS* eine Abteilung (z.B. *DeptX*) auswählen (1) und die zugehörigen Knoten *DeptX – Authorization Roles* aufklappen, werden die Benutzerrollen angezeigt (2), die für diese Abteilung (hier: *DeptX*) definiert sind.

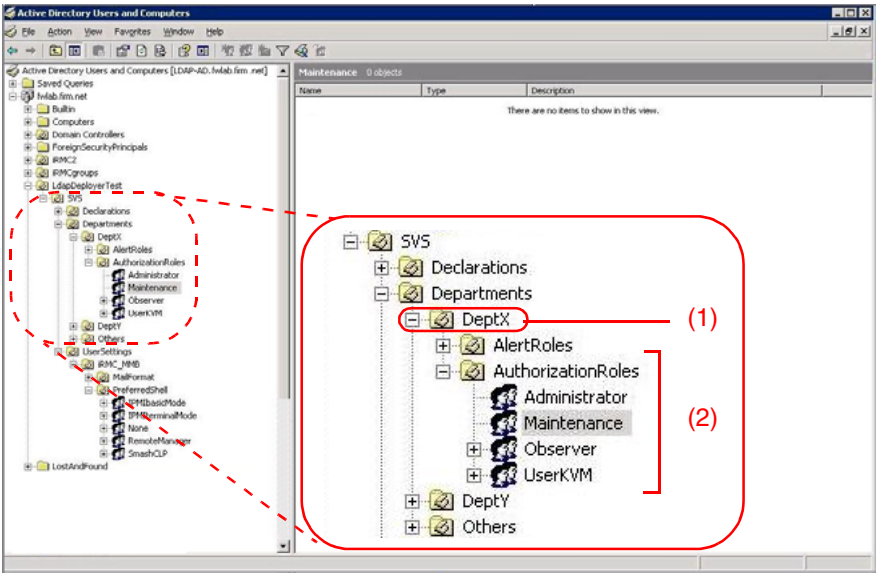


Bild 39: Anzeige der Benutzerrollen im Snap-in „Benutzer und -Computer

Berechtigungsgruppen anzeigen, denen ein Benutzer zugeordnet ist

Wenn Sie im Strukturbaum von *Active Directory Users and Computers*(siehe Bild 40) unter *Benutzer* einen Benutzer (z.B. *kvms4*) auswählen (1) und via Kontextmenü *Eigenschaften – Mitglieder* den *Eigenschaften*-Dialog für diesen Benutzer öffnen, werden in der Registerkarte *Mitglieder* die Berechtigungsgruppen angezeigt (2), denen der Benutzer (hier: *kvms4*) angehört.

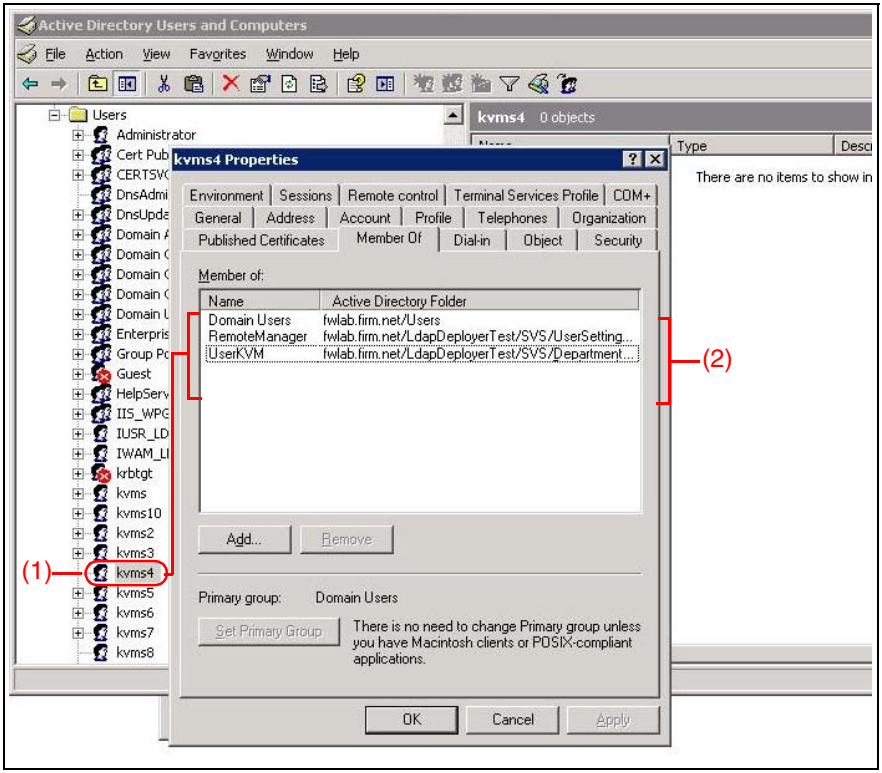


Bild 40: Eigenschaften-Dialog des Benutzers kvms4

7.2.3 SVS_LdapDeployer - Strukturen „SVS“ und „iRMCgroups“ generieren, pflegen und löschen

Um die globale iRMC S2/S3-Benutzerverwaltung über einen Verzeichnisdienst abwickeln zu können, müssen im LDAP-Verzeichnisdienst die Struktur(en) (OU) *SVS* und *iRMCgroups* angelegt sein.

Zum Generieren sowie zum Anpassen von *SVS*-Strukturen verwenden Sie den *SVS_LdapDeployer*. Der *SVS_LdapDeployer* ist ein Java-Archiv (*SVS_LdapDeployer.jar*), das Sie im Firmware-Package auf Ihrer ServerView Suite DVD finden.

Dieser Abschnitt beschreibt:

– Konfigurationsdatei des *SVS_LdapDeployer*

– *SVS_LdapDeployer*

– Kommandos und Optionen des *SVS_LdapDeployer*

– Typische Anwendungsszenarien

7.2.3.1 Konfigurationsdatei (xml-Datei)

SVS_LdapDeployer erzeugt LDAP-Strukturen auf Basis einer *xml*-Konfigurationsdatei. Diese Eingabedatei enthält die Strukturinformationen für die Struktur(en) *SVS* und/oder *iRMCgroups* in xml-Syntax.

Die Syntax der Konfigurationsdatei ersehen Sie aus den Beispiel-Konfigurationsdateien *Generic_Settings.xml* und *Generic_InitialDeploy.xml*, die Sie zusammen mit dem *jar*-Archiv *SVS_LdapDeployer.jar* auf der ServerView Suite DVD ausgeliefert werden.

In der Eingabedatei müssen unter <Settings> immer gültige Verbindungsdaten für die Verbindung zum Verzeichnisserver eingetragen sein.

Optional können Sie auch die Authentisierungsdaten für den Server-Zugriff eintragen. Alternativ können Sie die Authentisierungsdaten auch in der Kommandozeile des *SVS_LdapDeloyer* angeben.

Wenn Sie die Authentisierungsdaten weder in der Konfigurationsdatei noch in der Kommandozeile beim Aufruf des *SVS_LdapDeployer* angeben, fordert der *SVS_LdapDeployer* die Authentisierungsdaten zum Ausführungszeitpunkt an.

7.2.3.2 SVS_LdapDeployer starten

Zum Starten des *SVS_LdapDeployer* gehen Sie wie folgt vor:

- Speichern Sie das Java-Archiv (*jar*-Archiv) *SVS_LdapDeployer.jar* in ein Verzeichnis auf dem Verzeichnisserver.
- Öffnen Sie die Kommando-Schnittstelle des Verzeichnisservers.
- Wechseln Sie in das Verzeichnis, in dem das *jar*-Archiv *SVS_LdapDeployer.jar* gespeichert ist.
- Rufen Sie den *SVS_LdapDeployer* gemäß dem folgenden Syntax-Schema auf:

```
java –jar SVS_LdapDeployer.jar <kommando> <datei>
                                                [<option>...]
```

Während der Ausführung des *SVS_LdapDeployer* werden Sie über die durchgeführten Schritte informiert. Detaillierte Informationen finden Sie in der Datei *log.txt*, die bei jeder Ausführung des *SVS_LdapDeployer* im Ausführungsverzeichnis angelegt wird.

Im Folgenden werden die Begriffe "LDAPv1-Struktur" und "LDAPv2-Struktur" für die Bezeichnung ServerView-spezifischer Konfigurationslayouts der Autorisierungsdaten verwendet und beziehen sich nicht auf die Versionen 1 und 2 des LDAP-Protokolls.

Die Kommandos *-import* und *-sychronize* (siehe unten) werden nur in Verbindung mit LDAPv1-Strukturen benötigt (iRMC S2s mit einer Firmware-Version < 3.77 und iRMCs). Näheres hierzu finden Sie in den Handbüchern

- "iRMC S2/S3 - integrated Remote Management Controller", Ausgabe Mai 2011 und frühere Ausgaben.
- "iRMC - integrated Remote Management Controller"

<kommando>

Spezifiziert die durchzuführende Aktion.

Folgende Kommandos stehen zur Auswahl:

-deploy

Erzeugt auf dem Verzeichnisserver eine LDAP-Struktur für die globale iRMC S2/S3-Benutzerverwaltung (siehe Seite 165).

-delete
: Löscht auf dem Verzeichnisserver eine vorhandenen LDAP-Struktur, die für die globale iRMC / iRMC S2/S3-Benutzerverwaltung verwendet wird (siehe Seite 167).

-import
: Erzeugt aus einer existierenden LADAP v1-Struktur eine äquivalente LDAP v2-Struktur (siehe Seite 165).

-synchronize
: Zieht Änderungen, die Sie in einer LDAP v2-Struktur vornehmen, in einer bereits vorhandenen LDAP v1-Struktur nach (siehe Seite 165).

<datei>
: Konfigurationsdatei (*.xml*), die von *SVS_LdapDeploy* als Eingabedatei verwendet wird. Die Konfigurationsdatei enthält die Strukturinformationen für die Struktur(en) *SVS* und/oder *iRMCgroups* in *xml*-Syntax.

Die Syntax der Konfigurationsdatei ersehen Sie aus den Beispiel-Konfigurationsdateien *Generic_Settings.xml* und *Generic_InitialDeploy.xml*, die zusammen mit dem *jar*-Archiv *SVS_LdapDeployer.jar* auf der ServerView Suite DVD ausgeliefert wird.

<option> [<option> ...]
: Option(en), die die Ausführung des spezifizierten Kommandos steuern.

In den nachfolgenden Abschnitten werden die einzelnen Kommandos des *SVS_LdapDeployer* samt den zugehörigen Optionen im Detail erläutert.

Der *SVS_LdapDeployer* erzeugt alle benötigten Unterbäume inklusive aller Gruppen, nicht jedoch die Beziehungen zwischen Benutzern und Gruppen.

Die Erstellung und Zuordnung von Benutzereinträgen zu Gruppen nehmen Sie über ein entsprechendes Tool des verwendeten Verzeichnisdienstes vor, nachdem Sie die OUs *SVS* und/oder *iRMCgroups* im Verzeichnisdienst generiert haben.

7.2.3.3 -deploy: LDAP-Struktur erzeugen oder ändern

Mit dem Kommando *-deploy* können Sie auf dem Verzeichnisserver eine neue LDAP-Struktur erzeugen oder zu einer bereits existierende LDAP-Struktur neue Einträge hinzufügen.

> **i** Zum Entfernen von Einträgen aus einer existierenden LDAP-Struktur, müssen Sie die LDAP-Struktur zuerst mit *-delete* löschen (siehe Seite 167) löschen und anschließend mit einer entsprechend modifizierten Konfigurationsdatei neu generieren.

Syntax:

```
-deploy <datei> [-structure {v1 | v2 | both}]
      [ -username <benutzer>]
      [ -password <passwort>][ -store_pwd <pfad>][ -kloc <pfad>]
      [ -kpwd [<key-passwort>]]
```

<datei>
xml-Datei, die die Konfigurationsdaten enthält.

> **i** Die Konfigurationsdatei muss unter <Data> alle erforderlichen Rollen und Abteilungen enthalten, die für das erstmalige Generieren bzw. die Erweiterung einer Struktur benötigt werden.

-structure v1 | -structure v2 | -structure both
Erzeugt eine LDAP v1-Struktur oder eine LDAP v2-Struktur oder eine LDAP v1- und eine LDAP v2-Struktur.

-username <benutzer>
Benutzername zur Anmeldung am Verzeichnisserver.

-password <passwort>
Passwort für den Benutzer <benutzer>

-store_pwd

Verschlüsselt das Passwort <passwort> mithilfe eines zufallsgenerierten Schlüssels und speichert das verschlüsselte Passwort nach erfolgreicher Ausführung von *-deploy* in der Konfigurationsdatei ab. Der zufallsgenerierte Schlüssel wird standardmäßig in dem Ordner abgespeichert, in dem der *SVS_LdapDeployer* ausgeführt wird.

ACHTUNG!

Den zufallsgenerierten Schlüssel sollten Sie sicher abspeichern. Falls der voreingestellte Zielordner Ihren Sicherheitserfordernissen nicht genügt oder der Ordner, in dem der Schlüssel gespeichert wird, auch anderen Benutzern zugänglich ist, verwenden Sie für eine sichere Speicherung des Schlüssels die Optionen *-kloc* und *-kpwd*.

-kloc <pfad>

Speichert den zufallsgenerierten Schlüssel unter <pfad>.
Wenn Sie diese Option nicht angeben, wird der Schlüssel im dem Ordner gespeichert, in dem der *SVS_LdapDeployer* ausgeführt wird.

-kpwd [<passwort>]

Legt ein Passwort zum Schutz des zufallsgenerierten Schlüssels fest.
Wenn Sie <passwort> nicht angeben, wird das Passwort automatisch auf Basis einer Momentaufnahme der aktuellen Ablaufumgebung gebildet.

7.2.3.4 -delete: LDAP-Struktur löschen

Mit dem Kommando *-delete* können Sie auf dem Verzeichnisserver eine LDAP-Struktur entfernen.

Syntax:

```
-delete <datei> [-structure {v1 | v2 | both}]
      [ -username <benutzer>]
      [ -password <passwort>][ -store_pwd <pfad>][ -kloc <pfad>]
      [ -kpwd [<key-passwort>]]
```

<datei>
xml-Datei, die die zu löschende Struktur spezifiziert.

-structure v1 | -structure v2 | -structure both
Löscht LDAP v1-Struktur oder LDAP v2-Struktur oder LDAP v1- und LDAP v2-Struktur.

-username <benutzer>
Benutzername zur Anmeldung am Verzeichnisserver

-password <passwort>
Passwort für den Benutzer <benutzer>

-stor_pwd
Verschlüsselt das Passwort <passwort> mithilfe eines zufallsgenerierten Schlüssels und speichert das verschlüsselte Passwort nach erfolgreicher Ausführung von *-delete* in der Konfigurationsdatei ab. Der zufallsgenerierte Schlüssel wird standardmäßig in dem Ordner abgespeichert, in dem der *SVS_LdapDeployer* ausgeführt wird.

ACHTUNG!

Den zufallsgenerierten Schlüssel sollten Sie sicher abspeichern. Falls der voreingestellte Zielordner Ihren Sicherheitserfordernissen nicht genügt oder der Ordner, in dem der Schlüssel gespeichert wird, auch anderen Benutzern zugänglich ist, verwenden Sie für eine sichere Speicherung des Schlüssels die Optionen *-kloc* und *-kpwd*.

-kloc <pfad>
Speichert den zufallsgenerierten Schlüssel unter <pfad>.
Wenn Sie diese Option nicht angeben, wird der Schlüssel im dem Ordner gespeichert, in dem der *SVS_LdapDeployer* ausgeführt wird.

-kpwd [<passwort>]
Legt ein Passwort zum Schutz des zufallsgenerierten Schlüssels fest. Wenn Sie <passwort> nicht angeben, wird das Passwort automatisch auf Basis einer Momentaufnahme der aktuellen Ablaufumgebung gebildet.

7.2.4 Typische Anwendungsszenarien

Im Folgenden sind vier typische Szenarien für den Einsatz des *SVS_LdapDeployer* beschrieben.

7.2.4.1 Erst-Konfiguration einer LDAP v2-Struktur durchführen

Sie wollen erstmals die globale Benutzerverwaltung für einen iRMC S2/S3 (Firmware-Version 3.77 oder höher) einrichten. Hierfür benötigen Sie eine LDAP v2-Struktur.

Empfohlene Vorgehensweise:

Generieren Sie eine Department-Definition für LDAP v2-Strukturen (*SVS*):

```
java -jar SVS_LdapDeployer.jar -deploy myInitialDeploy.xml
     -structure v2
```

7.2.4.2 LDAP v2-Struktur neu generieren oder erweitern

Sie wollen eine LDAP v2-Struktur neu generieren oder eine bereits bestehende LDAP v2-Struktur erweitern.

Empfohlene Vorgehensweise:

```
java -jar SVS_LdapDeployer.jar -deploy myInitialDeploy.xml
     -structure -structure v2
```

oder

```
java -jar SVS_LdapDeployer.jar -deploy myInitialDeploy.xml
```

7.2.4.3 LDAP v2-Struktur neu generieren und Authentisierungsdaten anfordern und speichern

Sie wollen eine LDAP v2-Struktur neu generieren. Die Authentisierungsdaten sollen via Kommandozeile bereitgestellt und gespeichert werden.

Empfohlene Vorgehensweise:

```
java –jar SVS_LdapDeployer.jar –deploy myInitialDeploy.xml
     –store_pwd –username admin –password admin
```

Nach dem Speichern der Anmeldedaten können Sie sich über den *SVS_LdapDeployer* ohne Angabe von Benutzerkennung und Passwort mit dem Verzeichnisserver verbinden. Der *SVS_LdapDeployer* verwendet dann - sofern vorhanden - die in der xml-Konfigurationsdatei gespeicherten Werte. Ein gespeichertes Passwort kann der *SVS_LdapDeployer* nur dann verwenden, wenn er es entschlüsseln kann. Dies erfordert, dass Sie den *SVS_LdapDeployer* in derselben Laufzeitumgebung aufrufen, wie beim vorangegangenen Aufruf mit *-store_pwd* (siehe Seite 166). „Dieselbe Laufzeitumgebung“ bedeutet hier „derselbe Benutzer am selben Computer“ oder „Benutzer mit Zugriffsberechtigung auf das Verzeichnis, unter dem der Schlüssel gespeichert ist (Option *-kloc*, siehe Seite 166)“.

Für zukünftige Aufrufe des *SVS_LdapDeployer* können Sie auch Benutzerkennungen verwenden, die bereits gespeichert sind. Darüber hinaus lassen sich durch explizite Angabe in der Kommandozeile oder auf Anforderung durch den *SVS_LdapDeployer* zeitweilig auch andere Authentisierungsdaten nutzen.

7.2.5 iRMC S2/S3-Benutzerverwaltung via Microsoft Active Directory

Dieser Abschnitt beschreibt, wie Sie die iRMC S2/S3-Benutzerverwaltung in Microsoft Active Directory integrieren.

Voraussetzung:

Eine LDAP v2-Struktur ist im Active Directory-Verzeichnisdienst generiert (siehe Abschnitt "SVS_LdapDeployer - Strukturen „SVS“ und „iRMCgroups“ generieren, pflegen und löschen" auf Seite 162).

Zur Integration der iRMC S2/S3-Benutzerverwaltung in Microsoft Active Directory führen Sie die folgenden Schritte durch:

1. LDAP/SSL-Zugriff des iRMC S2/S3 am Active Directory Server konfigurieren.
2. iRMC S2/S3-Benutzer den iRMC S2/S3-Benutzergruppen in Active Directory zuordnen.

7.2.5.1 LDAP/SSL-Zugriff des iRMC S2/S3 am Active Directory Server konfigurieren

Die iRMC S2/S3-LDAP-Integration verwendet die auf dem OpenSSL Project basierende SSL Implementation von Eric Young. Einen Abdruck des SSL Copyrights finden Sie auf Seite 227.

Die Nutzung von LDAP via SSL durch den iRMC S2/S3 erfordert die Erstellung eines RSA-Zertifikats.

Die Konfiguration des LDAP-Zugriffs umfasst die folgenden Schritte:

1. Enterprise CA installieren.
2. RSA-Zertifikat für den Domänencontroller (Domain Controller) erzeugen.
3. RSA-Zertifikat auf dem Server installieren.

Enterprise CA installieren

Eine CA ist eine „Zertifizierungsstelle für Zertifikate“. Eine Enterprise CA („Zertifizierungsstelle für Unternehmen“) können Sie wahlweise auf dem Domänencontroller selbst oder auf einem anderen Server installieren.

Die Installation direkt auf dem Domänencontroller ist einfacher, da im Vergleich zur Installation auf einem anderen Server einige Installationsschritte entfallen.

Im Folgenden ist beschrieben, wie Sie die Enterprise CA direkt auf einem vom Domänencontroller verschiedenen Server installieren.

Die erfolgreiche Installation und Konfiguration einer Enterprise CA setzt eine Active Directory-Umgebung sowie die installierten IIS (**I**nternet **I**nformation **S**ervices) voraus.

Mit den folgenden Schritten installieren Sie eine Enterprise CA:

- Wählen Sie im Windows Startmenü:

  Start - Systemsteuerung - Software - Windows-Komponenten hinzufügen/entfernen

- Wählen Sie im Wizard für die Windows-Komponenten unter *Komponenten* den Punkt *Zertifikatsdienste*.

- Führen Sie einen Doppelklick auf *Zertifikatsdienste* aus und stellen Sie sicher, dass die Optionen *Webregistrierung für Zertifikatsdienste* und *Zertifizierungsstelle für Zertifikate* ausgewählt sind.

- Wählen Sie *Stammzertifizierungsstelle eines Unternehmens*.

- Aktivieren Sie die Option *Schlüsselpaar und Zertifizierungsstellenzertifikat mit diesen Einstellungen erstellen*.
- Wählen Sie *Microsoft Base DSS Cryptographic Provider*, um DSA-Zertifikate mit einer Schlüssellänge von 1024 Byte zu generieren.
- Exportieren Sie das öffentliche Zertifizierungsstellenzertifikat (CA Certificate).

  Im Einzelnen verfahren Sie hierfür wie folgt:

  - Starten Sie die Management-Konsole durch Eingabe von *mmc* in der Windows Eingabeaufforderung.
  - Fügen Sie das Snap-in für Zertifikate des lokalen Computers hinzu.
  - Navigieren Sie zu *Zertifikate (Lokaler Computer) - Vertrauenswürdige Stammzertifizierungsstellen - Zertifikate* und führen Sie einen Doppelklick aus.
  - Führen Sie einen Doppelklick auf das Zertifikat der neu erstellten Zertifizierungsstelle aus.
  - Klicken Sie im Zertifikatsfenster auf die Registerkarte *Details*.
  - Klicken Sie auf *In Datei kopieren*.
  - Wählen Sie einen Dateinamen für das Zertifizierungsstellenzertifikat und klicken Sie auf *Fertig stellen*.
- Laden Sie das öffentliche Zertifizierungsstellenzertifikat auf dem Domänencontroller in das Zertifikatsverzeichnis *Vertrauenswürdige Stammzertifizierungsstellen*.

  Im Einzelnen verfahren Sie hierfür wie folgt:

  - Übertragen Sie die Datei des Zertifizierungsstellenzertifikats auf den Domänencontroller.
  - Öffnen Sie im Windows Explorer das Zertifikat der neu erstellten Zertifizierungsstelle.
  - Klicken Sie auf *Zertifikat installieren*.
  - Klicken Sie unter *Alle Zertifikate in folgenden Speicher speichern* auf *Durchsuchen* und wählen Sie *Vertrauenswürdige Stammzertifizierungsstellen*.
  - Starten Sie die Management-Konsole durch Eingabe von *mmc* in der Windows Eingabeaufforderung.

- ► Fügen Sie das Snap-in für Zertifikate des lokalen Computers hinzu.
- ► Fügen Sie das Snap-in für Zertifikate des aktuellen Benutzers hinzu.
- ► Kopieren Sie das Zertifizierungsstellenzertifikat (CA Certificate) aus dem Verzeichnis *Vertrauenswürdige Stammzertifizierungsstellen* des aktuellen Benutzers in das Verzeichnis *Vertrauenswürdige Stammzertifizierungsstellen* des lokalen Computers.

Domänencontroller-Zertifikat erzeugen

Mit den folgenden Schritten erstellen Sie ein RSA-Zertifikat für den Domänencontroller:

► Erstellen Sie eine Datei *request.inf* mit dem folgenden Inhalt:

```
[Version]
Signature="$Windows NT$"
[NewRequest]
Subject = "CN=<full path of domain controller host>"
KeySpec = 1
KeyLength = 1024
Exportable = TRUE
MachineKeySet = TRUE
SMIME = FALSE
PrivateKeyArchive = FALSE
UserProtected = FALSE
UseExistingKeySet = FALSE
ProviderName = "Microsoft RSA SChannel Cryptographic
Provider"
ProviderType = 12
RequestType = PKCS10
KeyUsage = 0xa0

[EnhancedKeyUsageExtension]
OID=1.3.6.1.5.5.7.3.1
; this is for Server Authentication
```

► Passen Sie in der Datei *request.inf* die Angaben bei „Subject=“ an den Namen des verwendeten Domänencontrollers an, z.B. `Subject = "CN=domino.fwlab.firm.net".`

► Geben Sie in der Windows Eingabeaufforderung folgendes Kommando ein: *certreq -new request.inf request.req*

► Geben Sie im Browser der Zertifizierungsstelle folgende URL ein: *http://localhost/certsrv*

► Klicken Sie auf *Ein Zertifikat anfordern.*

- ► Klicken Sie auf *erweiterte Zertifikatsanforderung.*
- ► Klicken Sie auf *Reichen Sie eine Zertifikatsanforderung ein.*
- ► Kopieren Sie den Inhalt der Datei *request.req* in das Fenster *Gespeicherte Anforderungen*.
- ► Wählen Sie die Zertifikatsvorlage *Webserver*.
- ► Laden Sie das Zertifikat herunter und speichern Sie es ab (z.B. in der Datei *request.cer*).
- ► Geben Sie in der Windows Eingabeaufforderung folgendes Kommando ein: *certreq -accept request.cer*
- ► Exportieren Sie das Zertifikat mit dem privaten Schlüssel.

  Im Einzelnen verfahren Sie hierfür wie folgt:

  - ► Starten Sie die Management-Konsole durch Eingabe vom *mmc* in der Windows Eingabeaufforderung.
  - ► Fügen Sie das Snap-in für Zertifikate des lokalen Computers hinzu.
  - ► Navigieren Sie zu *Zertifikate (Lokaler Computer) - Eigene Zertifikate - Zertifikate*.
  - ► Führen Sie einen Doppelklick auf das neue Server-Authentifizierungszertifikat aus.
  - ► Klicken Sie im Zertifikatsfenster auf die Registerkarte *Details*.
  - ► Klicken Sie auf *In Datei kopieren.*
  - ► Wählen Sie *Ja, privaten Schlüssel exportieren*.
  - ► Vergeben Sie ein Passwort.
  - ► Wählen Sie einen Dateinamen für das Zertifikat und klicken Sie auf *Fertig stellen*.

Domänencontroller-Zertifikat auf dem Server installieren

Mit den folgenden Schritten installieren Sie das Domänencontroller-Zertifikat auf dem Server:

- ► Kopieren Sie die soeben erstellte Datei für das Domänencontroller-Zertifikat auf den Domänencontroller.
- ► Führen Sie einen Doppelklick auf das Domänencontroller-Zertifikat aus.
- ► Klicken Sie auf *Zertifikat installieren.*
- ► Verwenden Sie das Passwort, das Sie beim Export der Zertifikats vergeben haben.
- ► Klicken Sie unter *Alle Zertifikate in folgendem Speicher speichern* auf die Schaltfläche *Durchsuchen* und wählen Sie *Eigene Zertifikate*.
- ► Starten Sie die Management-Konsole durch Eingabe von *mmc* in der Windows Eingabeaufforderung.
- ► Fügen Sie das Snap-in für Zertifikate des lokalen Computers hinzu.
- ► Fügen Sie das Snap-in für Zertifikate des aktuellen Benutzers hinzu.
- ► Kopieren Sie das Domänencontroller-Zertifikat aus dem Verzeichnis *Eigene Zertifikate* des aktuellen Benutzers in das Verzeichnis *Eigene Zertifikate* des lokalen Computers.

7.2.5.2 iRMC S2/S3-Benutzer einer Rolle (Berechtigungsgruppe) zuordnen

Die Zuordnung von iRMC S2/S3-Benutzern zu iRMC S2/S3-Berechtigungsgruppen können Sie wahlweise vornehmen

– ausgehend vom Benutzereintrag oder
– ausgehend vom Rolleneintrag / Gruppeneintrag.

Nachfolgend ist am Beispiel der LDAP v2-Struktur die Zuordnung ausgehend vom Rolleneintrag anhand der OU *SVS* beschrieben. In der LDAP v1-Struktur sind die Gruppeneinträge in der OU *iRMCgroups* abgelegt.

Die Zuordnung ausgehend vom Benutzereintrag verläuft weitgehend analog.

In Active Directory müssen die Benutzer „von Hand“ in die Gruppen eingetragen werden.

Gehen Sie wie folgt vor:

► Öffnen Sie das Snap-in *Active Directory-Benutzer und -Computer*.

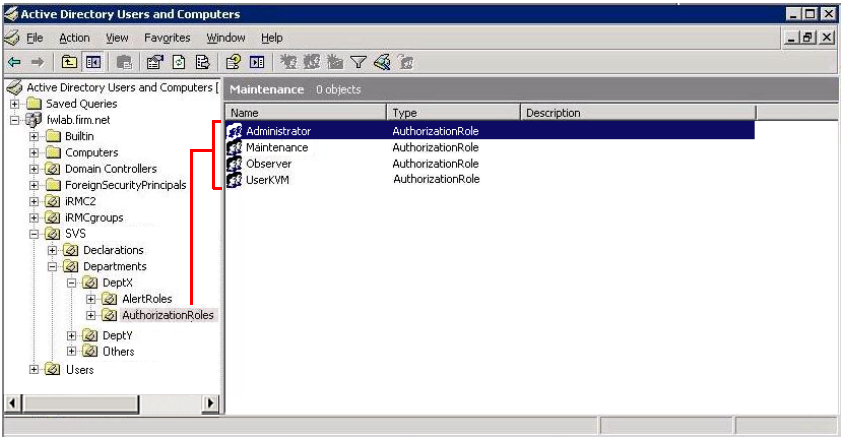


Bild 41: Snap-in Active Directory-Benutzer und -Computer

► Führen Sie einen Doppelklick auf die Berechtigungsgruppe (hier: Administrator) aus.

Der Dialog *Eigenschaften von Administrator* wird geöffnet (siehe Bild 42 auf Seite 177).

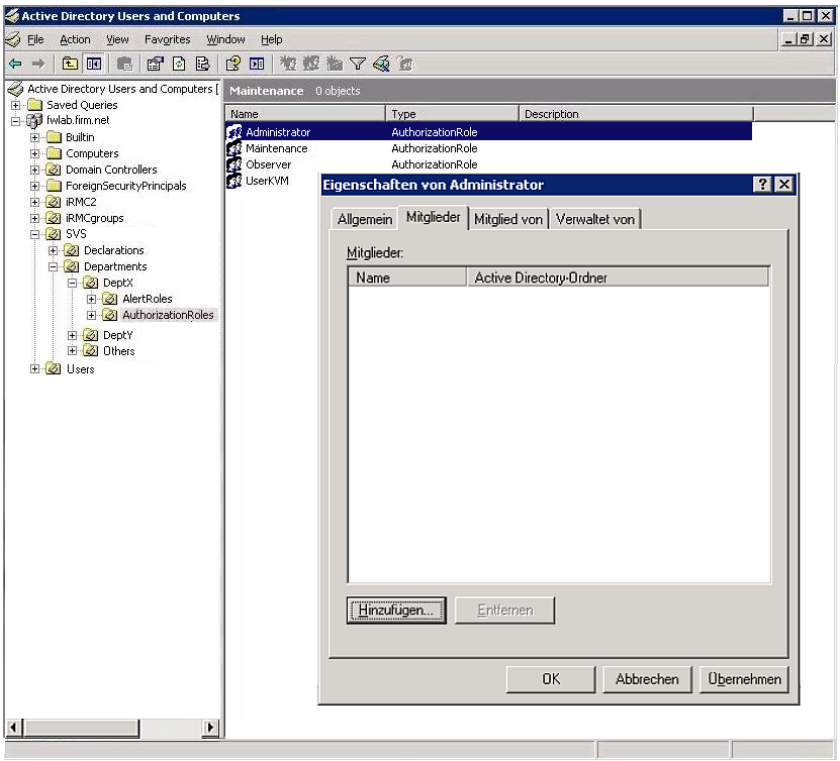


Bild 42: Dialog Eigenschaften von Administrator

- ► Wählen Sie die Registerkarte *Mitglieder*.
- ► Klicken Sie auf die Schaltfläche *Hinzufügen...* .

  Der Dialog *Benutzer, Kontakte oder Computer wählen* wird geöffnet (siehe Bild 43 auf Seite 178).

Bild 43: Dialog Benutzer, Kontakte oder Computer wählen

► Klicken Sie auf die Schaltfläche *Pfade...* .

Der Dialog *Pfad* wird geöffnet.

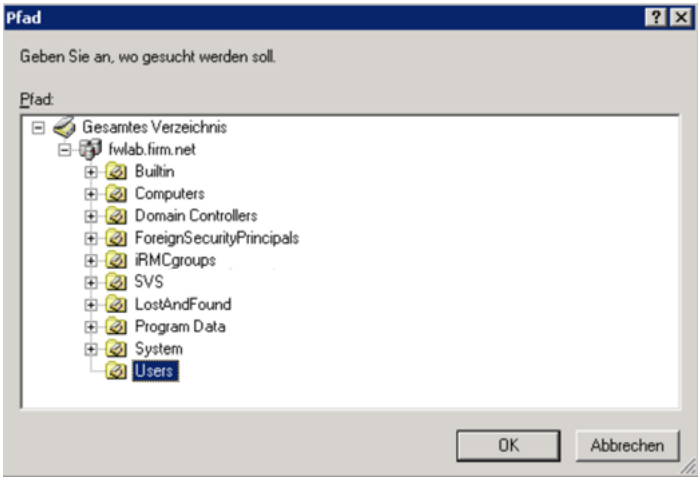


Bild 44: Dialog Pfad

► Wählen Sie den Container (OU), in dem sich Ihre Benutzer befinden. (Im Standardfall ist dies die OU *Users*.) Bestätigen Sie mit *OK*.

Der Dialog *Benutzer, Kontakte und Computer wählen* wird geöffnet (siehe Bild 45 auf Seite 179).

Benutzer können auch an anderer Stelle im Verzeichnis eingetragen sein.

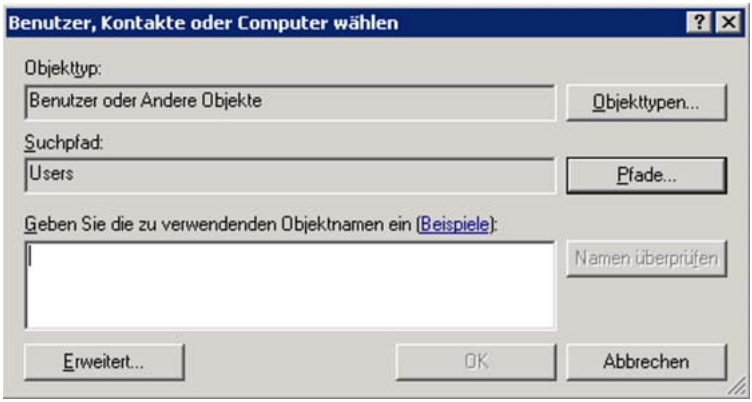


Bild 45: Dialog Benutzer, Kontakte oder Computer wählen

► Klicken Sie auf die Schaltfläche *Erweitert...* .

Ein erweiterter Dialog Benutzer, Kontakte und Computer wählen wird geöffnet (siehe Bild 46 auf Seite 180).

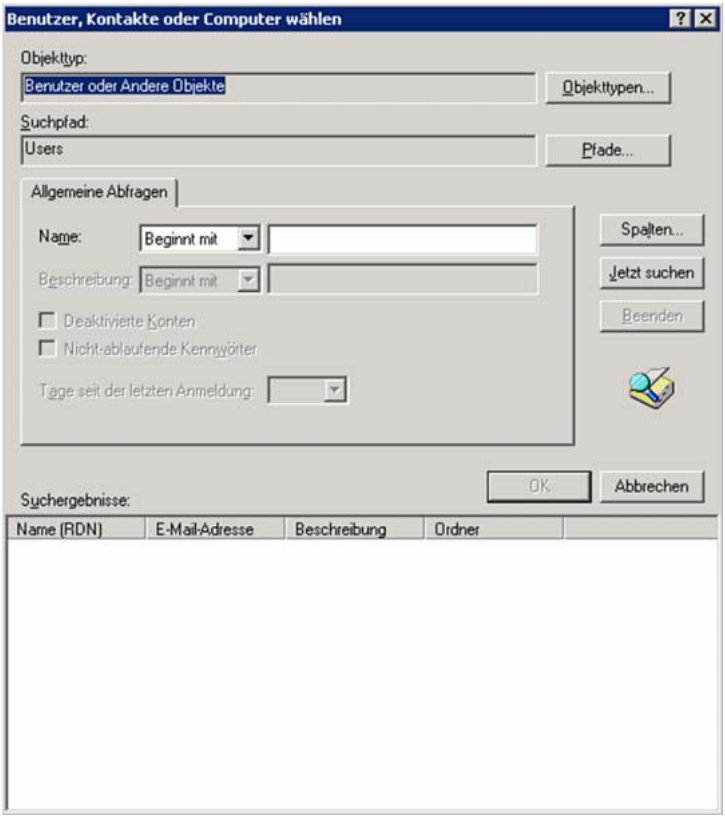


Bild 46: Dialog Benutzer, Kontakte oder Computer wählen - Suchen

► Klicken Sie auf die Schaltfläche *Jetzt suchen*, um sich alle Benutzer Ihrer Domäne anzeigen zu lassen.

Im Anzeigebereich unter *Suchergebnisse:* wird das Suchergebnis angezeigt (siehe Bild 47 auf Seite 181).

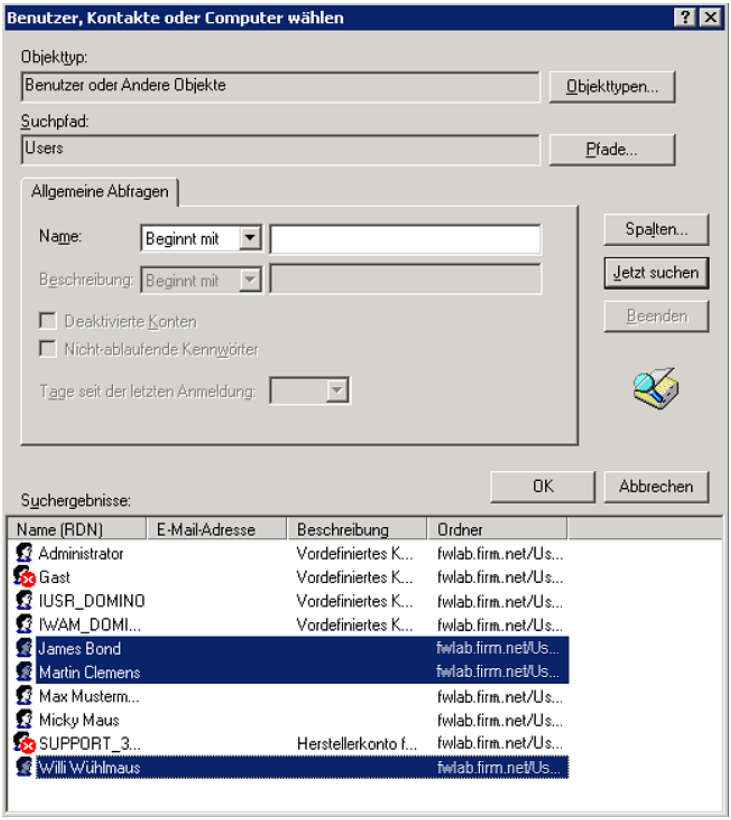


Bild 47: Dialog Benutzer, Kontakte oder Computer wählen - Suchergebnisse anzeigen

► Selektieren Sie die Benutzer, die zur Gruppe hinzugefügt werden sollen, und bestätigen Sie mit *OK*.

Es werden nun die ausgewählten Benutzer angezeigt (siehe Bild 48 auf Seite 182).

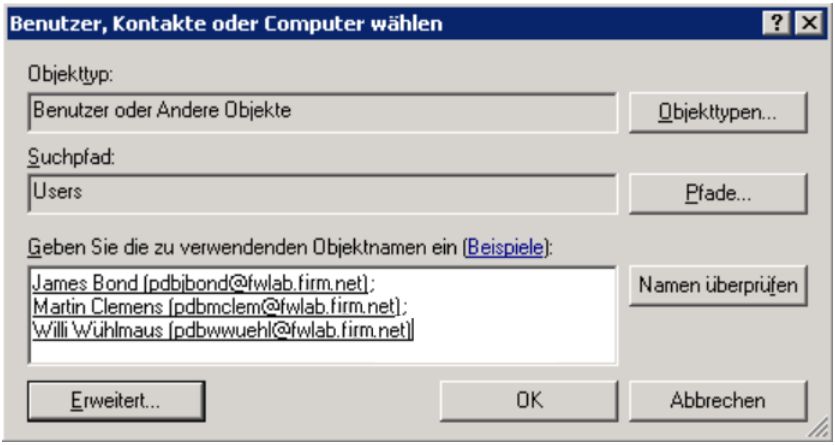


Bild 48: Dialog Benutzer, Kontakte oder Computer wählen - Suchergebnisse bestätigren

► Bestätigen Sie mit *OK*.

7.2.6 iRMC S2/S3-Benutzerverwaltung via Novell eDirectory

Dieser Abschnitt informiert über die folgenden Themen:

– Software-Komponenten und Systemanforderungen von Novell eDirectory

– Novell eDirectory installieren.

– Novell eDirectory konfigurieren.

– iRMC S2/S3-Benutzerverwaltung in Novell eDirectory integrieren.

– Tipps zur Administration von Novell eDirectory.

Installation und Konfiguration von Novell eDirectory werden im Folgenden ausführlich beschrieben. Tiefere eDirectory-Kenntnisse werden nicht vorausgesetzt. Sofern Sie bereits mit Novell eDirectory vertraut sind, können Sie die folgenden drei Abschnitte überspringen und fortfahren mit Abschnitt "iRMC S2/S3-Benutzerverwaltung in Novell eDirectory integrieren" auf Seite 197.

7.2.6.1 Software-Komponenten und Systemanforderungen

Verwenden Sie jeweils die angegebene oder eine aktuellere Version der nachfolgend aufgelisteten Komponenten.

Novell eDirectory (ehemals NDS) besteht aus folgenden Software-Komponenten:

– eDirectory 8.8: *20060526_0800_Linux_88-SP1_FINAL.tar.gz*

– eDirectory 8.8: *eDir_88_iMan26_Plugins.npm*

– iManager: *iMan_26_linux_64.tgz* für SuSE, *iMan_26_linux_32.tgz* sonst

– ConsoleOne: *c1_136f-linux.tar.gz*

Für Installation und Betrieb von Novell eDirectory gelten die folgenden Systemanforderungen:

– OpenSSL muss installiert sein.

  Falls OpenSSL nicht bereits installiert ist:

  ► Installieren Sie OpenSSL, **bevor** Sie mit der Installation von Novell eDirectory beginnen.

– 512 MB freier Hauptspeicher

7.2.6.2 Novell eDirectory installieren

Die Installation von Novell eDirectory umfasst die Installation der folgenden Komponenten:

– eDirectory Server und Administrations-Utilities

– iManager (Administrations-Utility)

– ConsoleOne (Administrations-Utility)

Voraussetzung für die Installation von Novell eDirectory:

– Ein Linux Server-Betriebssystem muss komplett installiert sein und laufen.

– Die Firewall muss für Verbindungen zu folgenden Ports konfiguriert sein: 8080, 8443, 9009, 81, 389, 636.

  Für OpenSuSE konfigurieren Sie dies mithilfe der Datei */etc/sysconfig/SuSEfirewall2*:

  ► Erweitern Sie in der Datei */etc/sysconfig/SuSEfirewall2* den Eintrag *FW_SERVICES_EXT_TCP* wie folgt:

  ```
  FW_SERVICES_EXT_TCP="8080 8443 9009 81 389 636"
  ```

– Gemäß dem eDirectory Installation Guide muss das System für Multicast Routing eingerichtet sein.

  Für SuSE Linux gehen Sie hierfür wie folgt vor:

  ► Erzeugen oder (sofern bereits vorhanden) öffnen Sie die Datei */etc/sysconfig/network/ifroute-eth0*.

  ► Erweitern Sie */etc/sysconfig/network/ifroute-eth0* um die folgende Zeile:

  ```
  224.0.0.0  0.0.0.0  240.0.0.0  eth0
  ```

  Dadurch passen Sie *eth0* der Systemkonfiguration an.

Voraussetzungen für die Installation des eDirectory Servers, der eDirectory Utilities, des iManager und von ConsoleOne:

- Für die Installation ist Root-Berechtigung erforderlich.
- Die im Folgenden beschriebene Vorgehensweise bei der Installation setzt voraus, dass alle für die Installation benötigten Dateien bereits in ein Verzeichnis (z.B. */home/eDirectory*) kopiert wurden. Es handelt sich dabei um folgende Dateien:

  20060526_0800_Linux_88-SP1_FINAL.tar.gz
  iMan_26_linux_64.tgz
  c1_136f-linux.tar.gz

eDirectory Server und Administrations-Utilities installieren

Gehen Sie wie folgt vor:

- Melden Sie sich mit Root-Berechtigung (Super User) an.
- Wechseln Sie in das Verzeichnis, das die für die Installation benötigten Dateien enthält (im Beispiel: */home/eDirectory*):

  ```
  cd /home/eDirectory
  ```

- Extrahieren Sie das Archiv *20060526_0800_Linux_88-SP1_FINAL.tar.gz*:

  ```
  tar -xzvf 20060526_0800_Linux_88-SP1_FINAL.tar.gz
  ```

  Nach der Extraktion enthält */home/eDirectory* ein neues Unterverzeichnis *eDirectory*.

eDirectory Server installieren

- Wechseln Sie in das Unterverzeichnis *setup* dieses *eDirectory*-Verzeichnisses:

  ```
  cd eDirectory/setup
  ```

- Rufen Sie das Installationsskript *./nds-install* auf:

  ```
  ./nds-install
  ```

- Akzeptieren Sie die EULA mit „y“ und bestätigen Sie mit der Enter-Taste.
- Wenn Sie nach dem zu installierenden Programm gefragt werden:

  Geben Sie „1“ ein für die **Installation des Novell eDirectory Servers** und bestätigen Sie mit der Enter-Taste.

  Daraufhin werden die eDirectory-Packages installiert.

Nach der Installation des Novell eDirectory Servers müssen Sie in einigen Umgebungsvariablen die Namen für die Pfade auf das eDirectory aktualisieren und die Variablen exportieren.

- Öffnen Sie hierfür Ihre Konfigurationsdatei (im Beispiel: */etc/bash.bashrc*) und fügen Sie die dort vor „# End of ...“ die folgenden Zeilen in der angegebenen Reihenfolge ein:

```
export PATH/opt/novell/eDirectory/bin:/opt/novell/eDirectory/
       sbin:$PATH

export LD_LIBRARY_PATH=/opt/novell/eDirectory/lib:/
       opt/novell/eDirectory/lib/nds-modules:/opt/novell/
       lib:$LD_LIBRARY_PATH

export MANPATH=/opt/novell/man:/opt/novell/eDirectory/
       man:$MANPATH

export TEXTDOMAINDIR=/opt/novell/eDirectory/share/
       locale:$TEXTDOMAINDIR
```

- Schließen Sie das Terminal und öffnen Sie ein neues Terminal, um die Umgebungsvariablen zu exportieren.

eDirectory Administrations-Utilities installieren

- Wechseln Sie in das Unterverzeichnis *setup* des *eDirectory*-Verzeichnisses:

```
cd eDirectory/setup
```

- Rufen Sie das Installationsskript auf:

```
./nds-install
```

- Akzeptieren Sie die EULA mit „y“ und bestätigen Sie mit der Enter-Taste.
- Wenn Sie nach dem zu installierenden Programm gefragt werden:

  Geben Sie „2“ ein für die **Installation der Novell eDirectory Administrations-Utilities** und bestätigen Sie mit der Enter-Taste.

  Daraufhin werden die eDirectory Administrations-Utilities installiert.

iManager installieren und aufrufen

Der iManager ist das für die Administration von Novell eDirectory empfohlene Tool. Für die Installation sowohl in SLES10 als auch in OpenSuSE verwenden Sie das Archiv **_64.tgz*.

Gehen Sie wie folgt vor:

- Melden Sie sich mit Root-Berechtigung (Super User) an.
- Wechseln Sie in das Verzeichnis */home/eDirectory*:

  ```
  cd /home/eDirectory
  ```

- Extrahieren Sie das Archiv *iMan_26_linux_64.tgz*:

  ```
  tar -xzvf iMan_26_linux_64.tgz
  ```

  Nach der Extraktion enthält */home/eDirectory* ein neues Unterverzeichnis *iManager*.

- Wechseln Sie in das Unterverzeichnis *installs* von *iManager*:

  ```
  cd iManager/installs/linux
  ```

- Rufen Sie das Installationsskript auf:

  ```
  ./iManagerInstallLinux.bin
  ```

- Wählen Sie die Sprache, in der die Installationsmeldungen ausgegeben werden sollen.
- Klicken Sie durch die EULA und akzeptieren Sie die EULA.
- Wählen Sie *1- Novell iManager 2.6, Tomcat, JVM* zur iManager-Installation.
- Wählen Sie *1- Yes* für Plugin-Download.
- Klicken Sie auf Enter, um den Default-Pfad für den Download zu verwenden.

  Das Installationsprogramm sucht via Internet nach Downloads. Dies kann einige Minuten dauern. Danach werden Sie aufgefordert, die zu installierenden Plugins auszuwählen.

  - Wählen Sie *All* für den Download aller Plugins.
  - Wählen Sie *1- Yes* für die Installation der lokal verfügbaren Plugins.

- Drücken Sie auf Enter, um den Default-Pfad für die Installation zu verwenden.
- Wählen Sie *2- No* für die automatische Konfiguration von Apache (optional).

- Akzeptieren Sie den Default Port (8080) für Tomcat.
- Akzeptieren Sie den Default SSL-Port (8443) für Tomcat.
- Akzeptieren Sie den Default JK Connector-Port (9009) für Tomcat.
- Geben Sie die administrationsberechtigte Benutzerkennung (z.B. „root.fts“) für den administrationsberechtigten Benutzer ein.
- Geben Sie den Baumnamen (z.B. „fwlab“) für den administrationsberechtigten Benutzer ein.
- Akzeptieren die aufgelistete Zusammenfassung Ihrer Eingaben mit *1-OK...*, um die Installation abzuschließen.

Beim Novell iManager einloggen

Nach der Installation können Sie sich via Web-Browser mithilfe der folgenden URL am iManager einloggen:

https://<IP-Adresse des eDirectory-Servers>:8443/nps

Novell empfiehlt die Verwendung der Web-Browser Microsoft Internet Explorer oder Mozilla Firefox. In Mozilla Firefox werden möglicherweise nicht alle Popup-Fenster des Kontext-Menüs angezeigt.

ConsoleOne installieren und starten

Mit ConsoleOne steht Ihnen ein weiteres Administrationstool von Novell eDirectory zur Verfügung.

Zur Installation von ConsoleOne gehen Sie wie folgt vor:

- Melden Sie sich mit Root-Berechtigung (Super User) am eDirectory Server an.
- Wechseln Sie in das Verzeichnis */home/eDirectory*:

  ```
  cd /home/eDirectory
  ```

- Extrahieren Sie das ConsoleOne-Archiv *c1_136f-linux.tar.gz*:

  ```
  tar -xzvf c1_136f-linux.tar.gz
  ```

  Nach der Extraktion enthält */home/eDirectory* ein neues Verzeichnis *Linux*.

- Wechseln Sie in das Verzeichnis *Linux*:

  ```
  cd Linux
  ```

- Rufen Sie das Installationsskript *c1-install* auf:

  ```
  ./c1-install
  ```

- Wählen Sie die Sprache, in der die Installationsmeldungen ausgegeben werden sollen.
- Geben Sie „8“ für die Installation aller Snap-Ins ein.

ConsoleOne benötigt den Pfad zu einer installierten Java-Laufzeitumgebung. Den entsprechenden Pfadnamen können Sie in die Umgebungsvariable *C1_JRE_HOME* exportieren. Demgegenüber erfordert der systemweite Export des Pfadnamens Änderungen in der *bash*-Profile.

Da Root-Berechtigung für das Arbeiten mit ConsoleOne erforderlich ist, genügt es im Prinzip, den Pfadnamen nur für die Kennung *superuser Root* zu exportieren. Im Folgenden ist jedoch der systemweite Export des Pfadnamens dargestellt. Damit können auch normale Benutzer mit ConsoleOne arbeiten, sofern sie Root-Berechtigung besitzen.

Gehen Sie wie folgt vor:

- Öffnen Sie die Ihre Konfigurationsdatei zur Bearbeitung (im Beispiel: */etc/bash.bashrc*)
- Fügen Sie in der Konfigurationsdatei vor „# End of ...“ die folgende Zeile ein:

```
export C1_JRE_HOME=/opt/novell/j2sdk1.4.2_05/jre
```

> **i** Hier wird die zusammen mit eDirectory installierte Java-Laufzeitumgebung verwendet. Sie können aber auch den Pfadnamen einer beliebigen anderen auf dem eDirectory Server installierten Java-Laufzeitumgebung angeben.

ConsoleOne erhält die verfügbaren Baumstrukturen entweder über die lokale Konfigurationsdatei *hosts.nds* oder über den SLP-Service und Multicast.

Zum Einfügen Ihrer Baumstruktur in die Konfigurationsdatei gehen Sie verfahren Sie wie folgt:

- Wechseln Sie in Ihr Konfigurationsverzeichnis:

```
cd /etc
```

- Erzeugen Sie die Datei *hosts.nds*, falls Sie noch nicht existiert.
- Öffnen Sie die Datei *hosts.nds* und fügen Sie die folgenden Zeilen ein:

```
#Syntax: TREENAME.FQDN:PORT
MY_Tree.mycomputer.mydomain:81
```

ConsoleOne starten

ConsoleOne starten Sie in der System-Eingabeaufforderung mit folgendem Kommando:

```
/usr/ConsoleOne/bin/ConsoleOne
```

7.2.6.3 Novell eDirectory konfigurieren

Zur Konfiguration von Novell eDirectory führen Sie die folgenden Schritte durch:

1. NDS-Baum erzeugen.
2. eDirectory für LDAP konfigurieren.
3. Zugang zu eDirectory via LDAP-Browser testen.

NDS-Baum erzeugen

Einen NDS (**N**etwork **D**irectory **S**ervice)-Baum erzeugen Sie mit dem Utility ndsmanage. ndsmanage benötigt hierfür die folgenden Informationen:

TREE NAME
: Netzweit eindeutiger Name für den neuen NDS-Baum, z.B. *MY_TREE*.

Server Name
: Name einer Instanz der Klasse *server* in eDirectory. Für *Server Name* spezifizieren Sie den Namen des PRIMERGY Servers, auf dem der LDAP-Server läuft, z.B. *lin36-root-0*.

Server Context
: Fully Distinguished Name (vollständige Beschreibung von Objektpfad und der Attributen) des Containers, in dem das *Server* Objekt enthalten ist, z.B. *dc=organization.dc=mycompany*.

Admin User
: Fully Distinguished Name (vollständige Beschreibung von Objektpfad und der Attributen) des administrationsberechtigten Benutzers, z.B. *cn= admin.dc=organization.dc=mycompany*

NCP Port
: Spezifizieren Sie den Port 81.

Instance Location
: Spezifizieren Sie als Pfad: */home/root/instance0*

Configuration File
: Spezifizieren Sie folgende Datei: */home/root /instance0/ndsconf*

Password for admin user
: Geben Sie hier das Administratorpasswort an.

Zur Konfigurierung des NDS-Baums gehen Sie wie folgt vor:

- ► Öffnen Sie eine Command Box.
- ► Wechseln Sie in das Verzeichnis */home/eDirectory*.
- ► Starten Sie das Utility ndsmanage durch Eingabe des Kommandos *ndsmanage*:

  ```
  ndsmanage
  ```

- ► Geben Sie „c“ ein für die Erzeugung einer neuen Instanz der Klasse *server*.
- ► Geben Sie „y“ ein , um die Konfiguration fortzusetzen.
- ► Geben Sie „y“ ein, um einen neuen Baum zu erzeugen.

  Anschließend erfragt ndsmanage nacheinander die Werte für *TREE NAME*, *Server Name*, *Server Context* etc. (siehe Seite 191).

  Sobald die Eingabe abgeschlossen ist, konfiguriert ndsmanage den NDS-Baum.

- ► Führen Sie nach Abschluss der Konfiguration des NDS-Baums einen Neustart des PRIMERGY Servers durch, um die Konfiguration zu aktivieren, d.h. den NDS-Baum zu erzeugen.

eDirectory für LDAP konfigurieren

Die Konfiguration von eDirectory für LDAP umfasst die folgenden Schritte:

- – Role Based Services (RBS) installieren.
- – Plugin-Module installieren.
- – Role Based Services (RBS) konfigurieren.
- – eDirectory mit/ohne SSL/TLS-Unterstützung konfigurieren.

Im Einzelnen gehen Sie wie folgt vor:

- ► Loggen Sie sich beim iManager via Web-Browser unter der Administratorkennung (*Admin*) ein.

Role Based Services (RBS) installieren

RBS installieren Sie mithilfe des iManager Configuration Wizard.

Gehen Sie wie folgt vor:

- Wählen Sie im iManager die Registerkarte *Configure* (durch Klicken auf das Desk-Symbol).
- Wählen Sie in der Registerkarte *Configure*:
  Role Based Services - *RBS Configuration*
- Starten Sie den RBS Configuration Wizard.
- Weisen *RBS2* dem zu verwaltenden Container zu. (Im obigen Beispiel ist dies „mycompany“.)

Plugin-Module installieren

Gehen Sie wie folgt vor:

- Wählen Sie im iManager die Registerkarte *Configure* (durch Klicken auf das Desk-Symbol).
- Wählen Sie in der Registerkarte *Configure*:
  Plug-in installation - *Available Novell Plug-in Modules*
- Wählen Sie in der Seite *Available Novell Plug-in Modules* unter den aufgelisteten Modulen das eDirectory-spezifische Package *eDir_88_iMan26_Plugins.npm*.
- Klicken Sie auf *Install*.

Role Based Services (RBS) konfigurieren

- Wählen Sie in der Seite *Available Novell Plug-in Modules* alle für die LDAP-Integration benötigten Module. Falls Sie sich nicht sicher sind, wählen Sie alle Module.
- Klicken Sie auf *Install*.

eDirectory für SSL/TLS gesicherten Zugriff konfigurieren

Während der eDirectory-Installation wird ein temporäres Zertifikat erzeugt, sodass der Zugriff auf eDirectory standardmäßig durch SSL/TLS abgesichert ist. Da jedoch die Firmware des iRMC S2/S3 für die Verwendung von RSA/MD5-Zertifikaten konfiguriert ist, benötigt die SSL/TLS gesicherte globale iRMC S2/S3-Benutzerverwaltung via eDirectory ein RSA/MD5 Zertifikat der Länge 1024 byte.

Ein RSA/MD5-Zertifikat der Länge 1024 byte erstellen Sie wie folgt mithilfe von ConsoleOne:

- Loggen Sie sich am LDAP-Server unter Ihrer Administratorkennung (*Admin*) ein und starten Sie ConsoleOne.
- Navigieren Sie zum Root-Verzeichnis Ihrer Unternehmensstruktur (z.B. *baumname/mycompany/myorganisation*).
- Wählen Sie *New Object - NDSPKI key material - custom*, um ein neues Objekt der Klasse *NDSPKI:Key Material* zu erstellen.
- Spezifizieren Sie im nachfolgenden Dialog die folgenden Werte:

  1. 1024 bits
  2. SSL or TLS
  3. signature RSA/MD5

  Ein neues Zertifikat des gewünschten Typs wird erstellt.

Um das neu erstellte Zertifikat für die SSL-gesicherte LDAP-Verbindung zu aktivieren führen Sie im iManager die folgenden Schritte durch:

- Starten Sie den iManager via Web-Browser.
- Loggen Sie sich beim iManager mit gültigen Authentisierungsdaten ein.
- Wählen Sie *LDAP - LDAP Options - LDAP Server - Connection*.

  Die Registerkarte *Connection* enthält eine Drop down-Liste, die alle auf dem System installierten Zertifikate anzeigt.
- Selektieren Sie in der Drop down-Liste das gewünschte Zertifikat.

eDirectory für den nicht-SSL-gesicherten Zugriff konfigurieren

Anonymes Login sowie die Übertragung von Klartext-Passwörtern über ungesicherte Kanäle sind in eDirectory standardmäßig deaktiviert. Demzufolge ist das Einloggen via Web-Browser am eDirectory-Server nur über eine SSL-Verbindung möglich.

Für die Nutzung von LDAP ohne SSL müssen Sie die folgenden Schritte durchführen:

1. Nicht-SSL-gesicherte LDAP-Verbindung ermöglichen.
2. Bind-Restriktionen lockern.
3. LDAP-Konfiguration neu laden.

Gehen Sie wie folgt vor:

1. Nicht-SSL-gesicherte LDAP-Verbindung ermöglichen.
   - ► Starten Sie den iManager via Web-Browser.
   - ► Loggen Sie sich beim iManager mit gültigen Authentisierungsdaten ein.
   - ► Wählen Sie den *Roles and Tasks*-View.
   - ► Wählen Sie *LDAP - LDAP Options - LDAP Server - Connection*.
   - ► Deaktivieren in der Registerkarte *Connection* die Option *Require TLS for all Operations.*
   - ► Wählen Sie *LDAP - LDAP Options - LDAP Group - General*.
   - ► Deaktivieren die in der Registerkarte *General* die Option *Require TLS for Simple Binds with password.*
2. Bind-Restriktionen lockern.
   - ► Loggen Sie sich beim iManager mit gültigen Authentisierungsdaten ein.
   - ► Navigieren Sie im Objekt-Baum zum *LDAP Server*-Objekt.
   - ► Markieren Sie das *LDAP Server*-Objekt per Maus-Klick und wählen Sie *Modify Object* im zughörigen Kontext-Menü.
   - ► Öffnen Sie im rechten Content-Frame das *Other*-Sheet.
   - ► Wählen Sie unter *Valued Attributes*: *ldapBindRestrictions*
   - ► Klicken Sie auf die Schaltfläche *Edit*.
   - ► Setzen Sie den Wertauf „0“.
   - ► Klicken Sie auf die Schaltfläche *OK*.
   - ► Klicken Sie im *Other*-Sheet auf die Schaltfläche *Apply*.
3. LDAP-Konfiguration neu laden.
   - ► Starten Sie ConsoleOne und loggen Sie sich in eDirectory ein.
   - ► Klicken Sie auf der links im Fenster auf das *Base DN*-Objekt (z.B. *Mycompany*). Auf der rechten Fensterseite wird daraufhin das *LDAP Server*-Objekt angezeigt.
   - ► Markieren Sie das *LDAP Server*-Objekt per Klick mit der rechten Maustaste und selektieren Sie *Properties...* im zughörigen Kontext-Menü.
   - ► Klicken Sie in der Registerkarte *General* auf *Refresh NLDAP Server Now*.

Zugriff auf eDirectory via LDAP Browser testen

Nach erfolgreicher Durchführung der oben beschriebenen Schritte 1 - 3 sollten Sie via LDAP Browser-Utility eine Verbindung zu eDirectory herstellen können. Mit dem LDAP-Browser von Jarek Gavor (siehe Seite 213) können Sie dies wie folgt testen:

- Versuchen Sie, sich unter der Administratorkennung (im Beispiel: *admin*) über eine SSL-Verbindung in eDirectory einzuloggen.

Falls der Versuch fehlschlägt, verfahren Sie wie folgt:

- Prüfen Sie, ob SSL aktiviert ist (vergleiche Seite 194).

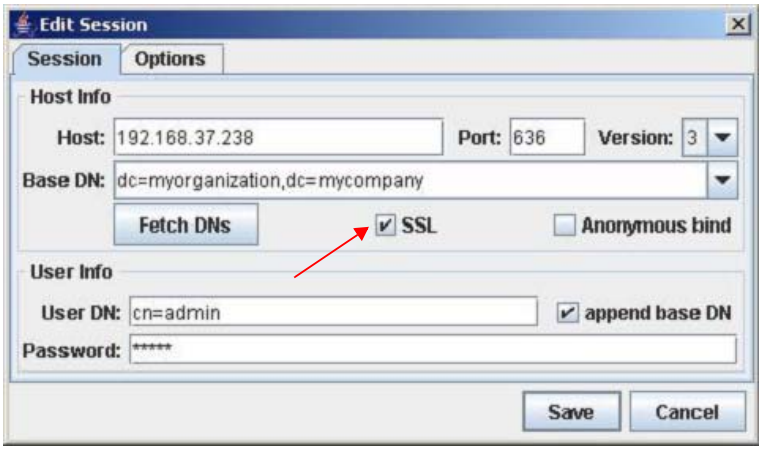


Bild 49: LDAP-Zugriff auf eDirectory testen: SSL aktiviert

- Versuchen Sie, sich unter der Administratorkennung (im Beispiel: *admin*) über eine nicht SSL-gesicherte Verbindung in eDirectory einzuloggen.

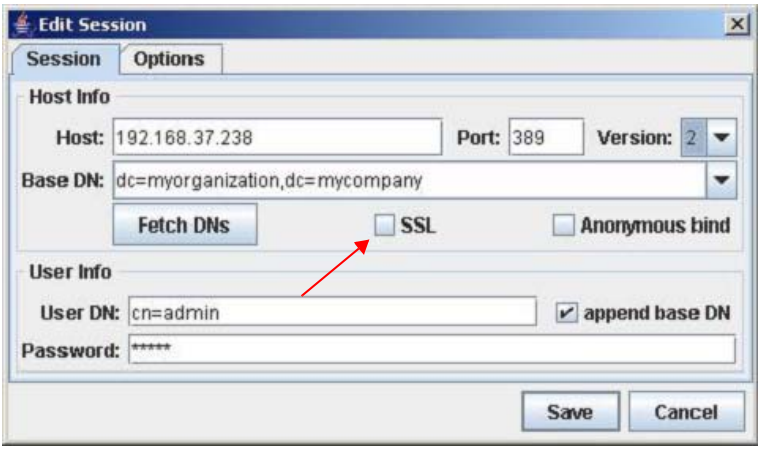


Bild 50: LDAP-Zugriff auf eDirectory testen: SSL nicht aktiviert

- Falls die Anmeldung erneut fehlschlägt:
  Lockern Sie die Bind-Restriktionen (siehe Seite 194).

7.2.6.4 iRMC S2/S3-Benutzerverwaltung in Novell eDirectory integrieren

Voraussetzung:

Eine LDAP v1 und/oder eine LDAP v2-Struktur ist im eDirectory-Verzeichnisdienst generiert (siehe Abschnitt "SVS_LdapDeployer - Strukturen „SVS“ und „iRMCgroups“ generieren, pflegen und löschen" auf Seite 162).

Für die Integration der iRMC S2/S3-Benutzerverwaltung in Novell eDirectory sind die folgenden Schritte erforderlich:

– Principal iRMC User erzeugen.

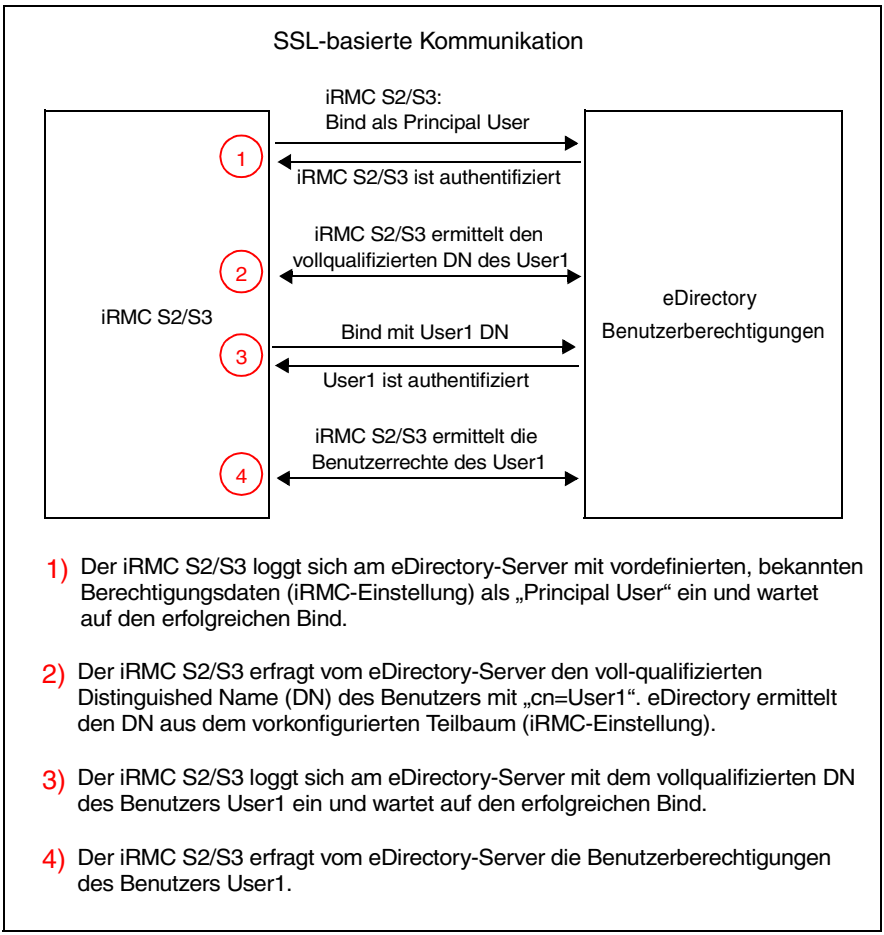
– iRMC-Gruppen und Benutzerrechte in eDirectory vereinbaren.

– Benutzer den Berechtigungsgruppen zuordnen.

LDAP-Authentifizierungsprozess für iRMC S2/S3-Benutzer in eDirectory

Die Authentifizierung eines globalen iRMC S2/S3-Benutzers beim Login am iRMC S2/S3 erfolgt nach einem fest vorgegebenen Schema (siehe Seite 150). Bild 51 auf Seite 198 veranschaulicht diesen Prozess für die globale iRMC S2/S3-Benutzerverwaltung mithilfe von Novell eDirectory.

Das Herstellen einer Verbindung und die Anmeldung mit entsprechenden Anmeldeinformationen wird als BIND-Operation bezeichnet.



1) Der iRMC S2/S3 loggt sich am eDirectory-Server mit vordefinierten, bekannten Berechtigungsdaten (iRMC-Einstellung) als „Principal User“ ein und wartet auf den erfolgreichen Bind.

2) Der iRMC S2/S3 erfragt vom eDirectory-Server den voll-qualifizierten Distinguished Name (DN) des Benutzers mit „cn=User1“. eDirectory ermittelt den DN aus dem vorkonfigurierten Teilbaum (iRMC-Einstellung).

3) Der iRMC S2/S3 loggt sich am eDirectory-Server mit dem vollqualifizierten DN des Benutzers User1 ein und wartet auf den erfolgreichen Bind.

4) Der iRMC S2/S3 erfragt vom eDirectory-Server die Benutzerberechtigungen des Benutzers User1.

Bild 51: Authentifizierungsschema für globale iRMC S2/S3-Benutzerberechtigungen

Die Berechtigungsdaten des „Principal User“ sowie den Teilbaum, der die DNs enthält, konfigurieren Sie in der Seite *Directory Service Configuration* der iRMC S2/S3-Web-Oberfläche (siehe Handbuch "iRMC S2/S3 - integrated Remote Management Controller").

Der CN eines Benutzers muss innerhalb des durchsuchten Teilbaums eindeutig sein.

Principal User (Principal Benutzer) für den iRMC S2/S3 erzeugen

Um einen Principal User für den iRMC S2/S3 zu erzeugen, gehen Sie wie folgt vor:

- Loggen Sie sich mit gültigen Authentisierungsdaten beim iManager ein.
- Wählen Sie *Roles and Tasks*.
- Wählen Sie *Users - Create User*.
- Tragen Sie die erforderlichen Angaben in das angezeigte Template ein.

  Distinguished Name (DN) und Passwort des Principal Users müssen mit entsprechenden Angaben für die Konfiguration des iRMC S2/S3 übereinstimmen (siehe Handbuch "iRMC S2/S3 - integrated Remote Management Controller").

  Der *Context:* des Benutzers kann sich an beliebiger Stelle im Baum befinden.

- Erteilen Sie dem Principal User Suchberechtigung für die folgenden Teilbäume:
  - Teilbaum (OU) *iRMCgroups* oder *SVS*
  - Teilbaum (OU), der die Benutzer enthält (z.B. *people*).

Den iRMC-Gruppen und -Benutzern Benutzerrechte erteilen

Standardmäßig verfügt ein Objekt in eDirectory nur über sehr eingeschränkte Abfrage- und Suchberechtigungen in einem LDAP-Baum. Damit ein Objekt alle Attribute in einem oder mehreren Teilbäumen abfragen kann, müsse Sie diesem Objekt die entsprechenden Rechte zuweisen.

Berechtigungen erteilen Sie wahlweise einem einzelnen Objekt (d.h. einem speziellen Benutzer) oder einer Gruppe von Objekten, die in einer Organizational Unit (OU) wie z.B. *SVS* oder *people* zusammengefasst sind. Dabei gehen Berechtigungen, die einer OU erteilt und als „inherited“ gekennzeichnet sind, automatisch auf die Objekte dieser Gruppe über.

Für die Integration der iRMC S2/S3-Benutzerverwaltung in Novell eDirectory ist es erforderlich, folgenden Objekten (Trustees) Suchberechtigung zu erteilen:

- *Principal User*
- Teilbaum, der die iRMC S2/S3-Benutzer enthält

Wie Sie dabei im Einzelnen vorgehen ist nachfolgend beschrieben.

Um einem Objekt die Suchberechtigung für alle Attribute zu erteilen, verfahren Sie wie folgt:

- Starten Sie den iManager via Web-Browser.
- Loggen Sie sich beim iManager mit gültigen Authentisierungsdaten ein.
- Klicken Sie im iManager auf die Schaltfläche *Roles and Tasks*.
- Wählen Sie im Menübaum *Rights - Rights to Other Objects*.

  Die Seite *Rights to Other Objects* wird angezeigt.
- Spezifizieren Sie unter *Trustee Name* den Namen des Objekts (in Bild 52 auf Seite 201 *iRMCgroups.sbrd4* und *SVS.sbdr4*), dem die Berechtigung erteilt werden soll.
- Spezifizieren Sie unter *Context to Search From* den eDirectory-Teilbaum (*iRMCgroups* / *SVS*), den der iManager nach allen Objekten durchsuchen soll, für die der Trustee *Users* zurzeit leseberechtigt ist.
- Klicken Sie auf die Schaltfläche *OK*.

  Eine Fortschrittanzeige informiert über den Stand der Suche. Nach Abschluss des Suchvorgangs wird die Seite *Rights to Other Objects* angezeigt, die jetzt das Suchergebnis enthält (siehe Bild 52 auf Seite 201).

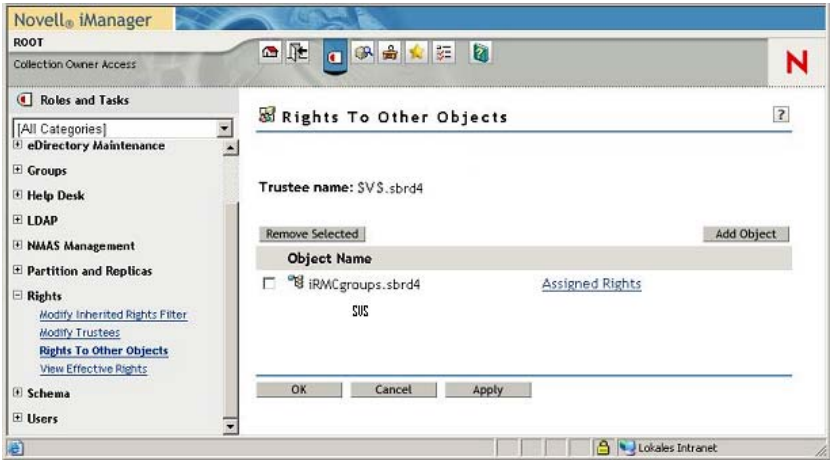


Bild 52: iManager - Roles and Tasks - Rights To Other Objects

Falls unter *Object Name* kein Objekt angezeigt wird, hat der Trustee zurzeit keine Berechtigung innerhalb des angegebenen Kontexts.

► Erteilen Sie dem Trustee gegebenenfalls zusätzliche Berechtigung(en):

► Klicken Sie auf *Add Object*.

► Selektieren Sie via Objektselektor-Schaltfläche das Objekt, für das Sie dem Trustee eine Berechtigung erteilen wollen.

► Klicken Sie auf *Assigned Rights*.

Falls die Property *[All Attributes Rights]* nicht angezeigt wird:

► Klicken Sie auf *Add Property*.

Das *Add Property*-Fenster wird angezeigt (siehe Bild 53 auf Seite 202).

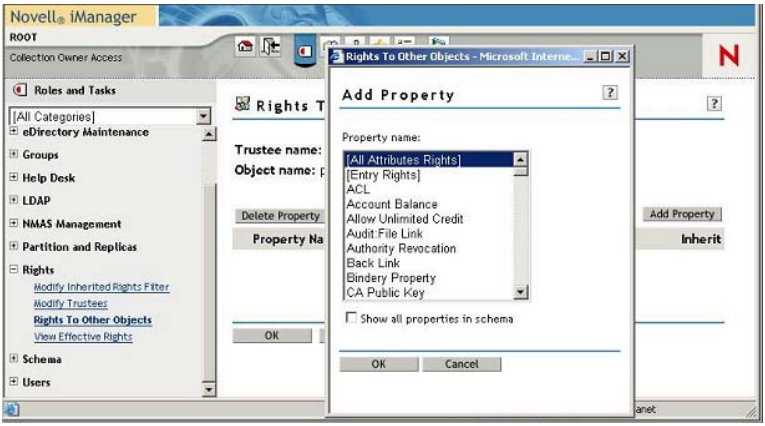


Bild 53: iManager - Roles and Tasks - Rights To Other Objects - Add Property

► Markieren Sie die Property *[All Attributes Rights]* und fügen Sie durch Klicken auf *OK* hinzu.

► Aktivieren Sie für die Property *[All Attributes Rights]* die Optionen *Compare*, *Read* und *Inherit* und bestätigen Sie mit *OK*.

Damit sind Benutzer/Benutzergruppe zur Abfrage aller Attribute im Teilbaum des ausgewählten Objekts autorisiert.

► Klicken Sie auf *Apply*, um Ihre Einstellungen zu aktivieren.

7.2.6.5 iRMC S2/S3-Benutzer der Berechtigungsgruppe zuordnen

Die Zuordnung von iRMC S2/S3-Benutzern (z.B. der OU *people*) zu iRMC S2/S3-Berechtigungsgruppen können Sie wahlweise vornehmen

– ausgehend vom Benutzereintrag (günstig bei wenigen Benutzereinträgen) oder
– ausgehend vom Rolleneintrag / Gruppeneintrag (günstig bei vielen Benutzereinträgen).

Nachfolgend ist exemplarisch die Zuordnung von iRMC S2/S3-Benutzern einer OU *people* zu einer Berechtigungsgruppe dargestellt. Erläutert wird dabei die vom Gruppeneintrag / Rolleneintrag ausgehende Zuordnung.

Die Zuordnung ausgehend vom Benutzereintrag verläuft weitgehend analog.

In eDirectory müssen die Benutzer „von Hand“ in die Gruppen eingetragen werden.

Gehen Sie wie folgt vor:

► Starten Sie den iManager via Web-Browser.

► Loggen Sie sich beim iManager mit gültigen Authentisierungsdaten ein.

► Wählen Sie *Roles and Tasks*.

► Wählen Sie *Groups - Modify Group*.

Die Seite *Modify Group* wird angezeigt.

► Führen Sie die folgenden Schritte für alle Berechtigungsgruppen durch, denen Sie iRMC S2/S3-Benutzer zuordnen wollen:

► Selektieren Sie via Objektselektor-Schaltfläche die Berechtigungsgruppe, der Sie iRMC S2/S3-Benutzer hinzufügen wollen (siehe Bild 54 auf Seite 204):
Administrator.AuthorizationRoles.DeptX.Departments.SVS.sbrd4

► Wählen Sie die Registerkarte *Members*.

Die Registerkarte *Members* der Seite *Modify Group* wird angezeigt:

Bild 54: iManager - Roles and Tasks - Modify Group - Registerkarte „Members“ (LDAP v2)

► Führen Sie den folgenden Schritt für alle Benutzer der OU *people* durch, die Sie der ausgewählten iRMC-Gruppe zuordnen wollen:

► Klicken Sie auf die Objektselektor-Schaltfläche .

Das *Object Selector (Browser)*-Fenster wird geöffnet (siehe Bild 55 auf Seite 205).

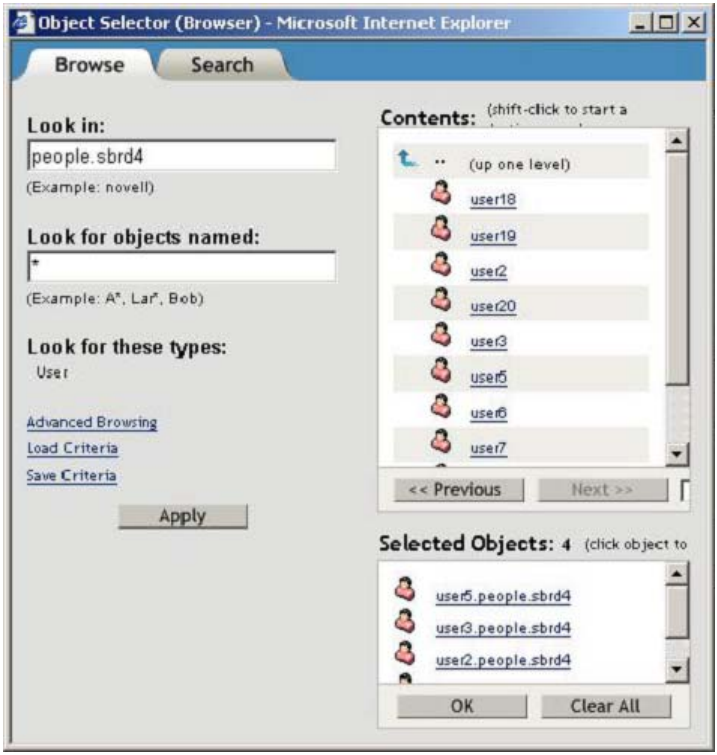


Bild 55: Benutzer der iRMC-Gruppe zuordnen - Benutzer auswählen

► Selektieren Sie im *Object Selector (Browser)*-Fenster den/die gewünschten Benutzer der OU *people* und bestätigen Sie Ihre Auswahl mit *OK*.

Im Anzeigebereich der Registerkarte *Members* der Seite *Modify Group* werden die ausgewählten Benutzer angezeigt (siehe 56 auf Seite 206).

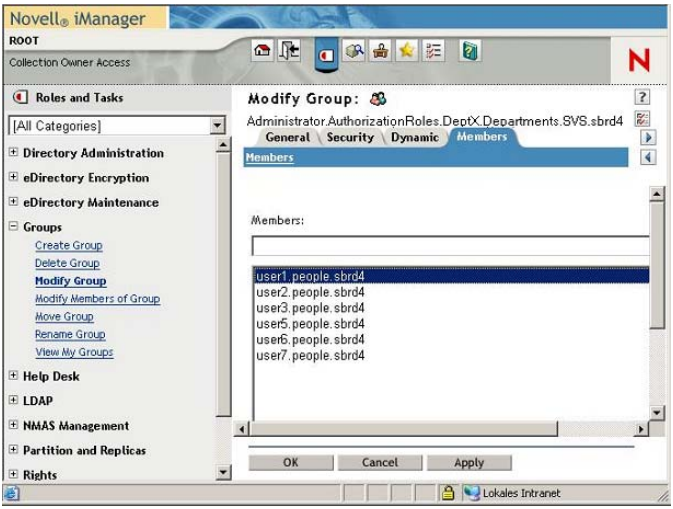


Bild 56: Anzeige der ausgewählten iRMC S2/S3-Benutzer in der Registerkarte „Members (LDAP v2)

► Bestätigen Sie mit *Apply* oder *OK*, um die ausgewählten Benutzer zur iRMC-Gruppe (hier: ... .*SVS.sbdr4*) hinzuzufügen.

7.2.6.6 Tipps zur Administration von Novell eDirectory

NDS-Dämon neu starten

Für einen Neustart des NDS-Dämons gehen Sie wie folgt vor:

- ► Öffnen Sie die Command Box.
- ► Melden Sie sich mit Root-Berechtigung an.
- ► Führen Sie das folgende Kommando aus:

```
rcndsd restart
```

Falls sich der nldap-Dämon ohne ersichtlichen Grund nicht starten lässt:

- ► Starten Sie den *lndap*-Dämon „von Hand“:

```
/etc/init.d/nldap restart
```

Falls der iManager nicht reagiert:

- ► Starten Sie den iManager neu:

```
/etc/init.d/novell-tomcat4 restart
```

Konfiguration des NLDAP-Servers neu laden

Gehen Sie wie folgt vor:

- ► Starten Sie ConsoleOne und loggen Sie sich in eDirectory ein.

  Wenn Sie ConsoleOne zum ersten Mal starten, ist noch kein Baum konfiguriert.

  Zur Konfiguration eines Baums gehen Sie wie folgt vor:

  - ► Wählen Sie unter *My World* den Knoten *NDS*.
  - ► Wählen Sie in der Menü-Leiste: *File - Authenticate*
  - ► Geben Sie für das Login die folgenden Authentisierungsdaten ein:
    1. Login-Name: root
    2. Passwort: <passwort>
    3. Tree: MY_TREE
    4. Context: mycompany

- ► Klicken Sie links im Fenster auf das *Base DN*-Objekt (*Mycompany*).

  Auf der rechten Fensterseite wird dann das *LDAP Server*-Objekt angezeigt.

- ► Klicken Sie mit der rechten Maustaste auf das *LDAP Server*-Objekt und wählen Sie *Properties...* im Kontext-Menü.

- ► Klicken Sie in der Registerkarte *General* auf die Schaltfläche *Refresh NLDAP Server Now*.

NDS Meldungs-Trace konfigurieren

Der *nds*-Dämon erzeugt Debug-und Log-Meldungen, die Sie mit dem Tool *ndstrace* verfolgen können. Zweck der im Folgenden beschriebenen Konfiguration ist es, den Terminal-Output von *ndstrace* in eine Datei umzuleiten und sich den Inhalt dieser Datei an einem anderen Terminal anzeigen zu lassen. Für Letzteres verwenden Sie das Tool *screen*.

Es empfiehlt sich folgende Vorgehensweise:

- ► Öffnen Sie die Command Box (z.B. *bash*).

ndstrace konfigurieren

- ► Wechseln Sie in das eDirectory-Verzeichnis */home/eDirectory*:

  ```
  cd /home/eDirectory
  ```

- ► Starten Sie *screen* mit dem Kommando `screen`.

- ► Starten Sie *ndstrace* mit dem Kommando `ndstrace`.

- ► Selektieren Sie die Module, die Sie aktivieren wollen.

  Wollen Sie sich z.B. die Zeitpunkte anzeigen lassen wollen, an denen Ereignisse eingetreten sind, dann geben Sie `dstrace TIME` ein.

  Es wird dringend empfohlen, die Module *LDAP* und *TIME* durch zu folgende Eingabe zu aktivieren:

  ```
  dstrace LDAP TIME
  ```

- ► Beenden *ndstrace* durch Eingabe von *quit*.

  Damit ist die Konfiguration von *ndstrace* abgeschlossen.

Meldungsausgabe auf zweites Terminal umleiten

- Starten Sie *ndstrace* und leiten Sie die Meldungsausgebe um:

  ```
  ndstrace -l >ndstrace.log
  ```

- Öffnen Sie ein zweites Terminal mithilfe der folgenden Tastenkombination: Ctrl + a, Crtl + c
- Schalten Sie den Mitschnitt der Protokollierung ein:

  ```
  tail -f ./ndstrace.log
  ```

- Um zwischen den virtuellen Terminals hin- und herzuschalten, verwenden Sie die Tastenkombination Ctrl + a, Crtl + 0.
  (Die Terminals sind von 0 bis 9 durchnummeriert.)

7.2.7 iRMC S2/S3-Benutzerverwaltung via OpenLDAP

Dieser Abschnitt informiert über die folgenden Themen:

– OpenLDAP installieren (Linux).

– SSL-Zertifikat erzeugen.

– OpenLDAP konfigurieren.

– iRMC S2/S3-Benutzerverwaltung in OpenLDAP integrieren.

– Tipps zur Administration von OpenLDAP

7.2.7.1 OpenLDAP installieren

Vor der Installation von OpenLDAP müssen Sie die Firewall für Verbindungen zu den Ports 389 und 636 konfigurieren.

Bei OpenSuSE verfahren Sie hierfür wie folgt:

► Ergänzen Sie in der Datei */etc/sysconfig/SuSEfirewall2* die Option *FW_SERVICES_EXT_TCP* wie folgt:

```
FW_SERVICES_EXT_TCP=“389 636“
```

Zur Installation der Packages *OpenSSL* und *OpenLDAP2* vom Distributionsmedium verwenden Sie das Setup-Tool YaST.

7.2.7.2 SSL-Zertifikate erzeugen

Es soll ein Zertifikat mit folgenden Eigenschaften erzeugt werden:

– Schlüssellänge: 1024 bit
– md5RSAEnc

Schlüsselpaare und signierte Zertifikate (selbstsigniert oder von einer externen CA signiert) erzeugen Sie mithilfe von OpenSSL. Nähere Informationen hierzu finden Sie auf der OpenSSL-Homepage unter *http://www.openssl.org*.

Unter den folgenden Links finden Sie Anleitungen zur Einrichtung einer CA und zum Erstellen von Test-Zertifikaten:

– *http://www.akadia.com/services/ssh_test_certificate.html*
– *http://www.freebsdmadeeasy.com/tutorials/web-server/apache-ssl-certs.php*
– *http://www.flatmtn.com/computer/Linux-SSLCertificates.html*
– *http://www.tc.umn.edu/~brams006/selfsign.html*

Als Ergebnis der Zertifikatserstellung müssen die folgenden drei PEM-Dateien vorliegen:

– Root-Zertifikat: *root.cer.pem*

– Server-Zertifikat: *server.cer.pem*

– Private Key: *server.key.pem*

Der Private Key **darf nicht** mit einer Passphrase verschlüsselt sein, da Sie **nur dem LDAP-Dämon** (*ldap*) Leseberechtigung für die Datei *server.key.pem* erteilen sollten.

Die Passphrase entfernen Sie mit folgendem Kommando:

```
openssl rsa -in server.enc.key.pem -out server.key.pem
```

7.2.7.3 OpenLDAP konfigurieren

Zur Konfiguration von OpenLDAP gehen Sie wie folgt vor:

- Starten Sie das Setup-Tool Yast und wählen Sie *LDAP-Server-Configuration*.
- Aktivieren Sie unter *Global Settings/Allow Settings* die Einstellung *LDAPv2-Bind*.
- Wählen Sie *Global Settings/TLS Settings*:
  - Aktivieren Sie die Einstellung *TLS*.
  - Geben Sie die Pfade der bei der Installation erstellten Dateien bekannt (siehe Abschnitt "OpenLDAP installieren" auf Seite 210).
  - Stellen Sie sicher, dass Zertifikate und Privater Schlüssel im Dateisystem vom LDAP-Service gelesen werden können.

    Da *openldap* unter der *uid/guid=ldap* ausgeführt wird, können Sie dies z.B. erreichen, indem Sie

    – den Eigentümer der Dateien mit Zertifikaten und privaten Schlüsseln auf „ldap“ setzen oder

    – dem LDAP-Dämon *ldap* die Leseberechtigung auf die Dateien mit Zertifikaten und privaten Schlüsseln erteilen.
- Wählen Sie *Databases*, um eine neue Datenbank zu erzeugen.

Falls die von YaST erstellte Konfiguration generell nicht funktioniert, prüfen Sie die Konfigurationsdatei */etc/openldap/slapd.conf* auf folgende zwingend erforderlichen Einträge:

```
allow bind_v2

TLSCACertificateFile /path/to/ca-certificate.pem

TLSCertificateFile /path/to/certificate.pem

TLSCertificateKeyFile /path/to/privat.key.pem
```

Falls die von YaST erstellte Konfiguration für SSL nicht funktioniert, prüfen Sie die Konfigurationsdatei */etc/sysconfig/openldap* auf folgenden Eintrag:

```
OPENLDAP_START_LDAPS=“yes“
```

7.2.7.4 iRMC S2/S3-Benutzerverwaltung in OpenLDAP integrieren

Voraussetzung:

Eine LDAP v1 und/oder eine LDAP v2-Struktur ist im OpenLDAP-Verzeichnisdienst generiert (siehe Abschnitt "SVS_LdapDeployer - Strukturen „SVS“ und „iRMCgroups“ generieren, pflegen und löschen" auf Seite 162).

Die Integration der iRMC S2/S3-Benutzerverwaltung in OpenLDAP umfasst die folgenden Schritte:

– Principal iRMC User erzeugen.

– Neuen iRMC S2/S3-Benutzer erzeugen und der Berechtigungsgruppe zuordnen.

Verwenden Sie zur Erzeugung des Principal User (ObjectClass: *Person*) einen LDAP-Browser, z.B. den LDAP Browser\Editor von Jarek Gawor (siehe Seite 213).

LDAP Browser\Editor von Jarek Gawor

Den LDAP Browser\Editor von Jarek Gawor können Sie über eine grafische Oberfläche einfach bedienen. Das Tool steht im Internet zum Download zur Verfügung.

Zur **Installation des LDAP Browser\Editor** verfahren Sie wie folgt:

- Entpacken Sie das Zip-Archiv *Browser281.zip* in ein Installationsverzeichnis Ihrer Wahl.
- Setzen Sie die Umgebungsvariable *JAVA_HOME* auf das Installationsverzeichnis der JAVA-Laufzeitumgebung, z. B.:

```
JAVA_HOME=C:\Programme\Java\jre7
```

Principal User (Principal Benutzer) erzeugen

Verwenden Sie zur Erzeugung des Principal User (ObjectClass: *Person*) einen LDAP-Browser, z.B. den LDAP Browser\Editor von Jarek Gawor (siehe Seite 213).

Im Folgenden ist beschrieben, wie Sie den Principal User mithilfe des LDAP Browser\Editor von Jarek Gawor erzeugen.

Gehen Sie wie folgt vor:

- Starten Sie den LDAP Browser.
- Loggen Sie sich beim OpenLDAP-Verzeichnisdienst mit gültigen Authentisierungsdaten ein.
- Wählen Sie den Teilbaum (Untergruppe), in dem der Principal User angelegt werden soll. Der Principal User kann an beliebiger Stelle dieses Baums angelegt werden.
- Öffnen Sie das Menü *Edit*.
- Wählen Sie *Add Entry*.
- Wählen Sie *Person*.
- Ändern Sie den Distinguished Name *DN*.

  Distinguished Name (DN) und Passwort des Principal User müssen mit entsprechenden Angaben für die Konfiguration des iRMC S2/S3 übereinstimmen (siehe Handbuch "iRMC S2/S3 - integrated Remote Management Controller").
- Klicken Sie auf *Set* und geben Sie ein Passwort ein.
- Geben Sie einen Sur Name *SN* ein.
- Klicken Sie auf *Apply*.

Neuen iRMC S2/S3-Benutzer erzeugen und den Berechtigungsgruppen zuordnen

Verwenden Sie für Erzeugung eines neuen Benutzers (ObjectClass *Person*) sowie zur Zuordnung eines Benutzers zur Berechtigungsgruppe einen LDAP-Browser, z.B. den LDAP Browser\Editor von Jarek Gawor (siehe Seite 213).

Im Folgenden ist beschrieben, wie Sie mithilfe des LDAP Browser\Editor von Jarek Gawor einen neuen iRMC S2/S3-Benutzer erzeugen und ihn zur Berechtigungsgruppe hinzufügen.

Gehen Sie wie folgt vor:

- Starten Sie den LDAP Browser.
- Loggen Sie sich beim OpenLDAP-Verzeichnisdienst mit gültigen Authentisierungsdaten ein.
- Erzeugen Sie einen neuen Benutzer:

  Gehen Sie hierbei wie folgt vor:

  - Wählen Sie den Teilbaum (Untergruppe), in dem der neue Benutzer angelegt werden soll. Der neue Benutzer kann an beliebiger Stelle des Baums angelegt werden.
  - Öffnen Sie das Menü *Edit*.
  - Wählen Sie *Add Entry*.
  - Wählen Sie *Person*.
  - Ändern Sie den Distinguished Name *DN*.
  - Klicken Sie auf *Set* und geben Sie das Passwort ein.
  - Geben Sie einen Sur Name *SN* ein.
  - Klicken Sie auf *Apply*.

► Ordnen Sie den soeben erzeugten Benutzer der Berechtigungsgruppe zu.

Gehen Sie hierbei wie folgt vor:

► Wählen Sie den Teilbaum (Untergruppe) von *iRMCgroups* oder *SVS*, dem der Benutzer angehören soll, d.h.

– *Für LDAP v1:*
cn=UserKVM,ou=YourDepartment,ou=Departments,ou=iRMCgroups, dc=myorganisation,dc=mycompany

– *Für LDAP v2:*
cn=UserKVM,ou=YourDepartment,ou=Departments,ou=SVS, dc=myorganisation,dc=mycompany

► Öffnen Sie das Menü *Edit*.

► Wählen Sie *Add Attribute*.

► Geben Sie als Attributnamen „Member“ ein. Als Wert geben Sie den vollqualifizierten DN zuvor erzeugten Benutzers an, also

cn=UserKVM,ou=YourDepartment,ou=Departments,ou=iRMCgroups, dc=myorganization,dc=mycompany

bzw.

cn=UserKVM,ou=YourDepartment,ou=Departments,ou=SVS, dc=myorganisation,dc=mycompany

7.2.7.5 Tipps zur Administration von OpenLDAP

LDAP-Service neu starten

Um den LDAP-Service neu zu starten, verfahren Sie wie folgt:

- Öffnen Sie die Command Box.
- Melden Sie sich mit Root-Berechtigung an.
- Geben Sie das folgende Kommando ein:

```
rcldap restart
```

Meldungsprotokollierung

Für das Meldungslogging nutzt der LDAP-Dämon das Syslog-Protokoll.

Die protokollierten Meldungen werden nur angezeigt, wenn in der Datei */etc/openldap/slapd.conf* ein Log-Level ungleich 0 eingestellt ist.

Erläuterungen zu den verschiedenen Leveln finden Sie unter:

http://www.zytrax.com/books/ldap/ch6/#loglevel

Tabelle 35 auf Seite 218 gibt einen Überblick über die Log-Level und ihre Bedeutung.

Log-Level	Bedeutung
-1	umfassendes Debugging
0	kein Debugging
1	Funktionsaufrufe protokollieren
2	Paketverarbeitung testen
4	Heavy Trace Debugging
8	Verbindungsmanagement
16	Gesendete und empfangene Pakete anzeigen
32	Suchfilterverarbeitung
64	Konfigurationsdateiverarbeitung
128	Verarbeitung der Zugangskontrolllisten
256	Status-Logging für Verbindungen / Operationen /Ergebnisse
512	Status-Logging für gesendete Einträge
1024	Kommunikation mit den Shell Backends ausgeben.
2048	Ergebnisse des Entry Parsings ausgeben.

Tabelle 35: OpenLDAP - Log-Level

7.2.8 E-Mail-Benachrichtigung an globale iRMC S2/S3-Benutzer konfigurieren

Die E-Mail-Benachrichtigung an globale iRMC S2/S3-Benutzer ist in die globale iRMC S2/S3-Benutzerverwaltung integriert und kann somit zentral und Plattform-übergreifend über einen Verzeichnisserver konfiguriert und abgewickelt werden. Entsprechend konfigurierte globale Benutzerkennungen können E-Mail-Benachrichtigungen von allen iRMC S2/S3 erhalten, die mit dem Verzeichnisserver im Netz verbunden sind.

Voraussetzungen

Für die E-Mail-Benachrichtigung müssen folgende Voraussetzungen erfüllt sein:

- Globale E-Mail-Benachrichtigung setzt eine iRMC S2/S3-Firmware der Version 3.77A oder höher voraus, da eine LDAP v2-Struktur benötigt wird.
- In der iRMC S2/S3-Web-Oberfläche muss ein Principal Benutzer konfiguriert sein, der berechtigt ist, im LDAP-Verzeichnisbaum (LDAP Tree) zu suchen (siehe Handbuch "iRMC S2/S3 - integrated Remote Management Controller").
- Bei der Konfiguration der LDAP-Einstellungen auf der Seite *Verzeichnisdienst Konfiguration* muss unter *Verzeichnisdienst E-Mail Benachrichtigung* die E-Mail-Benachrichtigung konfiguriert sein (siehe Handbuch "iRMC S2/S3 - integrated Remote Management Controller").

7.2.8.1 Globale E-Mail-Benachrichtigung

Die globale E-Mail-Benachrichtigung via Verzeichnisserver erfordert Benachrichtigungsgruppen (Alert Roles), die Sie zusätzlich zu den Authorization Roles in der Konfigurationsdatei des *SVS_LdapDeployer* (siehe Seite 162) definieren.

Benachrichtigungsgruppen (Alert Roles)

Eine Benachrichtigungsgruppe umfasst eine Auswahl definierter Benachrichtigungstypen (Alert Types, z.B. Temperaturüberschreitung) mit jeweils zugeordnetem Fehlergewicht (Severity, z.B. „kritisch“). Für Benutzer, die einer bestimmten Benachrichtigungsgruppe zugeordnet sind, legt die Benachrichtigungsgruppe fest, bei welchen Benachrichtigungstypen und Fehlergewichten die Benutzer per E-Mail benachrichtigt werden.

Die Syntax der Alert Roles ersehen Sie aus den Beispiel-Konfigurationsdateien *Generic_Settings.xml* und *Generic_InitialDeploy.xml*, die zusammen mit dem *jar*-Archiv *SVS_LdapDeployer.jar* auf der ServerView Suite DVD ausgeliefert werden.

Benachrichtigungstypen (Alert Types)

Folgende Benachrichtigungstypen werden unterstützt:

Benachrichtigungstyp	Ursache
FanSens	Lüfter-Sensoren
Temperat	Temperatur-Sensoren
HWError	Kritische Hardware-Fehler
Security	Sicherheit
SysHang	System-Hang
POSTErr	Systemstart-Fehler
SysStat	Systemstatus
DDCtrl	Festplatten und Controller
NetInterf	Netzwerk-Schnittstelle
RemMgmt	Remote Management
SysPwr	Energieverwaltung
Memory	Speicher
Others	Andere

Tabelle 36: Benachrichtigungstypen (Alert-Types)

Jedem Benachrichtigungstyp kann eines der folgenden Fehlergewichte (Severity Level) zugeordnet werden: *Warning*, *Critical*, *All*, (*none*).

Bevorzugter Mail Server

Bei globaler E-Mail-Benachrichtigung gilt für den bevorzugten Mail-Server die Einstellung *Automatic*: Falls die E-Mail nicht sofort erfolgreich versendet werden kann, weil z. B. der erste Mail-Server nicht verfügbar ist, wird E-Mail an den zweiten Mail-Server gesendet.

Unterstützte Mail-Formate

Es werden die folgenden Mail-Formate unterstützt:

– Standard
– Fixed Subject
– ITS-Format
– Fujitsu REMCS Format

Bei einem Mail-Format ungleich *Standard* müssen Sie die Benutzer der entsprechenden Mail-Format-Gruppe hinzufügen.

LDAP E-Mail-Tabelle

Wenn die E-Mail-Benachrichtigung konfiguriert ist (siehe Seite 223) und die Option *LDAP E-Mail aktiviert* gesetzt ist, sendet der iRMC S2/S3 im Fall einer Alarmbenachrichtigung E-Mails an (siehe auch Handbuch "iRMC S2/S3 - integrated Remote Management Controller").

– alle entsprechend konfigurierten lokalen iRMC S2/S3-Benutzer,

– alle globalen iRMC S2/S3-Benutzer, die in der LDAP E-Mail-Tabelle für diese Alarmbenachrichtigung registriert sind.

Die LDAP E-Mail-Tabelle wird in der iRMC S2/S3-Firmware erstmalig beim Erst-Start des iRMC S2/S3 angelegt und danach in regelmäßigen Abständen aktualisiert. Der Umfang der LDAP E-Mail-Tabelle ist begrenzt auf maximal 64 LDAP-Benachrichtigungsgruppen sowie auf maximal 64 globale iRMC S2/S3-Benutzer, für die E-Mail-Benachrichtigung konfiguriert ist.

Es wird empfohlen, für die globale E-Mail-Benachrichtigung Email-Verteiler zu verwenden.

Für die E-Mail-Benachrichtigung ermittelt der LDAP-Verzeichnisserver aus der E-Mail-Tabelle folgende Informationen:

- Liste der globalen iRMC S2/S3-Benutzer, für die E-Mail-Benachrichtigung konfiguriert ist.
- Für jeden globalen iRMC S2/S3-Benutzer:
  - Liste der konfigurierten Alarmbenachrichtigungen des jeweiligen Alerts (Art und Fehlergewicht)
  - Gewünschtes Mail-Format

Die LDAP E-Mail-Tabelle wird bei folgenden Anlässen aktualisiert:

- Erst-/Neustart des iRMC S2/S3
- Änderung der LDAP-Konfiguration
- In regelmäßigen Abständen (optional). Das Aktualiserungsintervall legen Sie bei der LDAP-Konfiguration in der iRMC S2/S3-Web-Oberfläche fest (Seite in der Option *LDAP E-Mail Tabellen aktualisieren* (siehe Handbuch "iRMC S2/S3 - integrated Remote Management Controller").

Globale E-Mail-Benachrichtigung auf dem Verzeichnisserver konfigurieren

Nachfolgend ist beschrieben, wie Sie die E-Mail-Benachrichtigung auf dem Verzeichnisserver konfigurieren.

Zusätzlich sind Einstellungen für den iRMC S2/S3 erforderlich, die Sie an der iRMC S2/S3-Web-Oberfläche konfigurieren (siehe Handbuch "iRMC S2/S3 - integrated Remote Management Controller").

Gehen Sie wie folgt vor:

- Tragen Sie im Verzeichnisdienst die E-Mail-Adressen der Benutzer ein, an die E-Mails gesendet werden sollen.

  Das Verfahren zur Konfiguration der E-Mail Adresse unterscheidet sich je nach verwendetem Verzeichnisdienst (Active Directory, eDirectory und OpenLdap).

- Erstellen Sie eine Konfigurationsdatei, in der die Alert Roles definiert sind.

- Starten Sie den *SVS_LdapDeployer* mit dieser Konfigurationsdatei, um eine entsprechende LDAP v2-Struktur (*SVS*) auf dem Verzeichnisserver zu generieren (siehe Seite 163 und Seite 169).

7.2.8.2 Benachrichtigungsgruppen (Alert Roles) anzeigen

Nach der Generierung der LDAP v2-Struktur wird z.B. in Active Directory die neu angelegte OU *SVS* mit den Komponenten *Alert Roles* und *Alert Types* unter *Declarations* sowie mit der Komponente *Alert Roles* unter *DeptX* angezeigt (siehe Bild 57):

– Unter *Declarations* zeigt *Alert Roles* alle definierten Alert Roles an, *Alert Types* werden alle Benachrichtigungstypen angezeigt (1).

– Unter *DeptX* zeigt *Alert Roles* alle in der OU *DeptX* gültigen Alert Roles an (2).

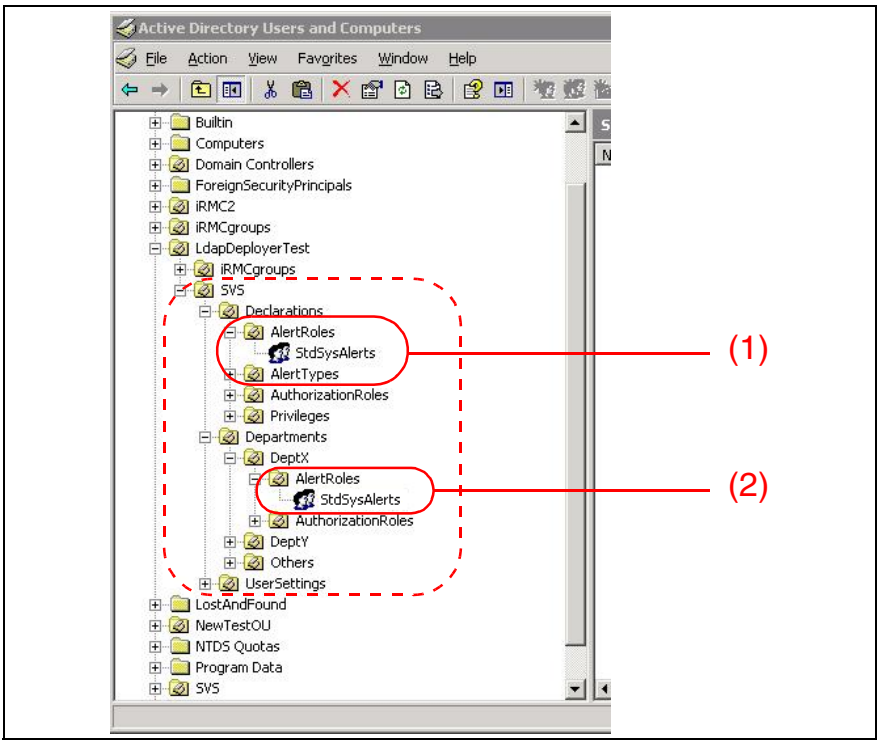


Bild 57: OU SVS mit Alert Roles

Damit an die Benutzer der einzelnen Benachrichtigungsgruppen E-Mails versendet werden, muss am iRMC S2/S3 die zugehörige Abteilung (Department, in Bild 57: *DeptX*) konfiguriert sein (siehe Handbuch "iRMC S2/S3 - integrated Remote Management Controller").

Wenn Sie im Strukturbaum von *Active Directory-Benutzer und -Computer* (siehe Bild 58) unter *SVS – Departments – DeptX – Alert Roles* eine Benachrichtigungsgruppe (Alert Role, z.B. *StdSysAlerts*) auswählen (1) und via Kontextmenü *Eigenschaften – Mitglieder* den *Eigenschaften*-Dialog für diese Benachrichtigungsgruppe öffnen, werden in der Registerkarte *Mitglieder* die Benutzer angezeigt (2), die der Benachrichtigungsgruppe (hier: *StdSysAlerts*) angehören.

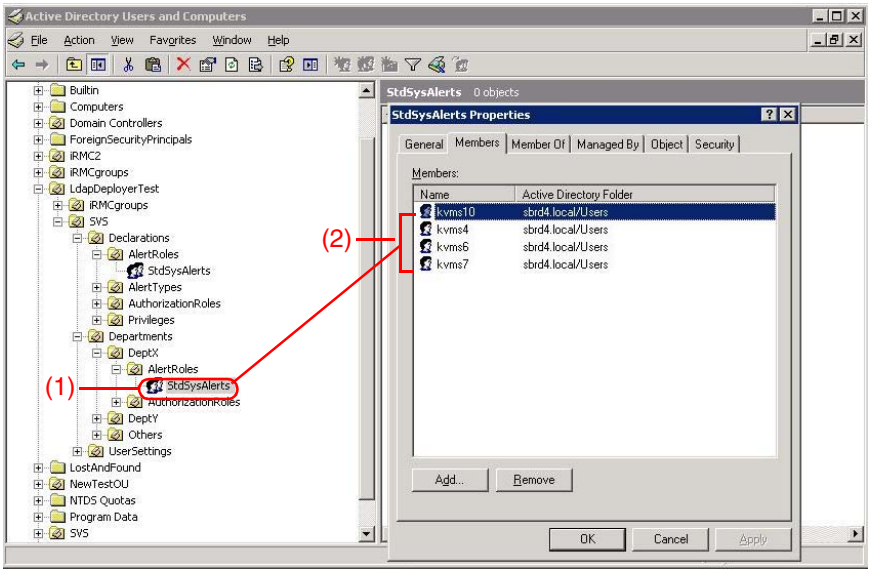


Bild 58: Benutzer mit der Alert Role „StdSysAlert“

7.2.8.3 iRMC S2/S3-Benutzer einer Benachrichtigungsgruppe (Alert Role) zuordnen

Die Zuordnung von iRMC S2/S3-Benutzern zu Benachrichtigungsgruppen (Alert Roles) können Sie wahlweise vornehmen

– ausgehend vom Benutzereintrag oder
– ausgehend vom Rolleneintrag.

In den einzelnen Verzeichnisdiensten (Microsoft Active Directory, Novell eDirectory und OpenLDAP) erfolgt die Zuordnung iRMC S2/S3-Benutzern zu iRMC S2/S3 Benachrichtigungsgruppen (Alert Roles) analog und mit denselben Tools wie bei der Zuordnung von iRMC S2/S3-Benutzern zu iRMC S2/S3-Berechtigungsgruppen (Authorization Roles).

In Active Directory z.B. treffen Sie die Zuordnung über die Schaltfläche *Add...* im *Eigenschaften*-Dialog des Snap-in *Active Directory Benutzer und -Computer* (siehe Bild 58 auf Seite 225).

7.2.9 SSL Copyright

Die iRMC S2/S3-LDAP Integration verwendet die auf dem OpenSSL Project basierende SSL Implementation von Eric Young.

```
/* ====================================================================
 * Copyright (c) 1998-2002 The OpenSSL Project.  All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 *
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in
 *    the documentation and/or other materials provided with the
 *    distribution.
 *
 * 3. All advertising materials mentioning features or use of this
 *    software must display the following acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
 *
 * 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
 *    endorse or promote products derived from this software without
 *    prior written permission. For written permission, please contact
 *    openssl-core@openssl.org.
 *
 * 5. Products derived from this software may not be called "OpenSSL"
 *    nor may "OpenSSL" appear in their names without prior written
 *    permission of the OpenSSL Project.
 *
 * 6. Redistributions of any form whatsoever must retain the following
 *    acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
 *
 * THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
 * EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
 * PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
 * ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
 * SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
 * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
 * LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
 * STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
 * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
 * OF THE POSSIBILITY OF SUCH DAMAGE.
 * ====================================================================
 *
 * This product includes cryptographic software written by Eric Young
 * (eay@cryptsoft.com).  This product includes software written by Tim
 * Hudson (tjh@cryptsoft.com).
 *
 */
```

```
/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
 * All rights reserved.
 *
 * This package is an SSL implementation written
 * by Eric Young (eay@cryptsoft.com).
 * The implementation was written so as to conform with Netscapes SSL.
 *
 * This library is free for commercial and non-commercial use as long as
 * the following conditions are aheared to.  The following conditions
 * apply to all code found in this distribution, be it the RC4, RSA,
 * lhash, DES, etc., code; not just the SSL code.  The SSL documentation
 * included with this distribution is covered by the same copyright terms
 * except that the holder is Tim Hudson (tjh@cryptsoft.com).
 *
 * Copyright remains Eric Young's, and as such any Copyright notices in
 * the code are not to be removed.
 * If this package is used in a product, Eric Young should be given attribution
 * as the author of the parts of the library used.
 * This can be in the form of a textual message at program startup or
 * in documentation (online or textual) provided with the package.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the copyright
 *    notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in the
 *    documentation and/or other materials provided with the distribution.
 * 3. All advertising materials mentioning features or use of this software
 *    must display the following acknowledgement:
 *    "This product includes cryptographic software written by
 *     Eric Young (eay@cryptsoft.com)"
 *    The word 'cryptographic' can be left out if the rouines from the library
 *    being used are not cryptographic related :-).
 * 4. If you include any Windows specific code (or a derivative thereof) from
 *    the apps directory (application code) you must include an acknowledgement:
 *    "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
 *
 * THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
 * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
 * ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
 * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
 * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
 * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
 * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
 * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
 * SUCH DAMAGE.
 *
 * The licence and distribution terms for any publically available version or
 * derivative of this code cannot be changed.  i.e. this code cannot simply be
 * copied and put under another distribution licence
 * [including the GNU Public Licence.]
 */
```

8 Anhang 2 - Globale iRMC S4-Benutzerverwaltung via Verzeichnisdienst

Die Benutzerverwaltung für den iRMC S4 verwendet zwei verschiedene Arten von Benutzerkennungen:

– **Lokale Benutzerkennungen** sind lokal im nicht-flüchtigen Speicher des iRMC S4 hinterlegt und werden über die Benutzerschnittstellen des iRMC S4 verwaltet.

– **Globale Benutzerkennungen** sind in der zentralen Datenhaltung eines Verzeichnisdienstes (Directory Service) hinterlegt und werden über die Schnittstellen dieses Verzeichnisdienstes verwaltet.

  Für die globale iRMC S4-Benutzerverwaltung werden zurzeit folgende Verzeichnisdienste unterstützt:

  – Microsoft® Active Directory
  – Novell® eDirectory
  – OpenLDAP
  – ForgeRock OpenDJ (Bei ServerView wird dieser Verzeichnisdienst im "embedded" Modus unter JBoss ausgeführt.)

Das vorliegende Kapitel informiert über folgende Themen:

– Konzept der Benutzerverwaltung für den iRMC S4
– Benutzerberechtigungen
– globale Benutzerverwaltung mithilfe der einzelnen Verzeichnisdienste

Einzelheiten zur lokalen Benutzerverwaltung des iRMC S4 finden Sie im Handbuch „iRMC S4 - integrated Remote Management Controller“.

In SeverView’s OpenDJ, ausgeführt im "embedded" Modus unter JBoss wird die Funktion *E-Mail-Einstellungen* des iRMC S4 nicht unterstützt.

8.1 Konzept der Benutzerverwaltung für den iRMC S4

Die Benutzerverwaltung für den iRMC S4 unterstützt die parallele Verwaltung lokaler und globaler Benutzerkennungen.

Bei der Validierung der Authentisierungsdaten (Benutzername, Passwort), die ein Benutzer beim Login an einer der iRMC S4-Schnittstellen eingibt, verfährt der iRMC S4 gemäß dem folgenden Ablauf (siehe auch Bild 59 auf Seite 231):

1. Der iRMC S4 gleicht den Benutzernamen und das Passwort mit den lokal gespeicherten Benutzerkennungen ab:
   - Bei erfolgreicher Authentifizierung des Benutzers durch den iRMC S4 (Benutzername und Passwort sind gültig) darf sich der Benutzer einloggen.
   - Andernfalls setzt der iRMC S4 die Prüfung mit Schritt 2. fort.
2. Der iRMC S4 authentisiert sich beim Verzeichnisdienst via LDAP mit Benutzernamen und Passwort, ermittelt per LDAP-Anfrage die Benutzerrechte und prüft, ob der Benutzer damit am iRMC S4 arbeiten darf.

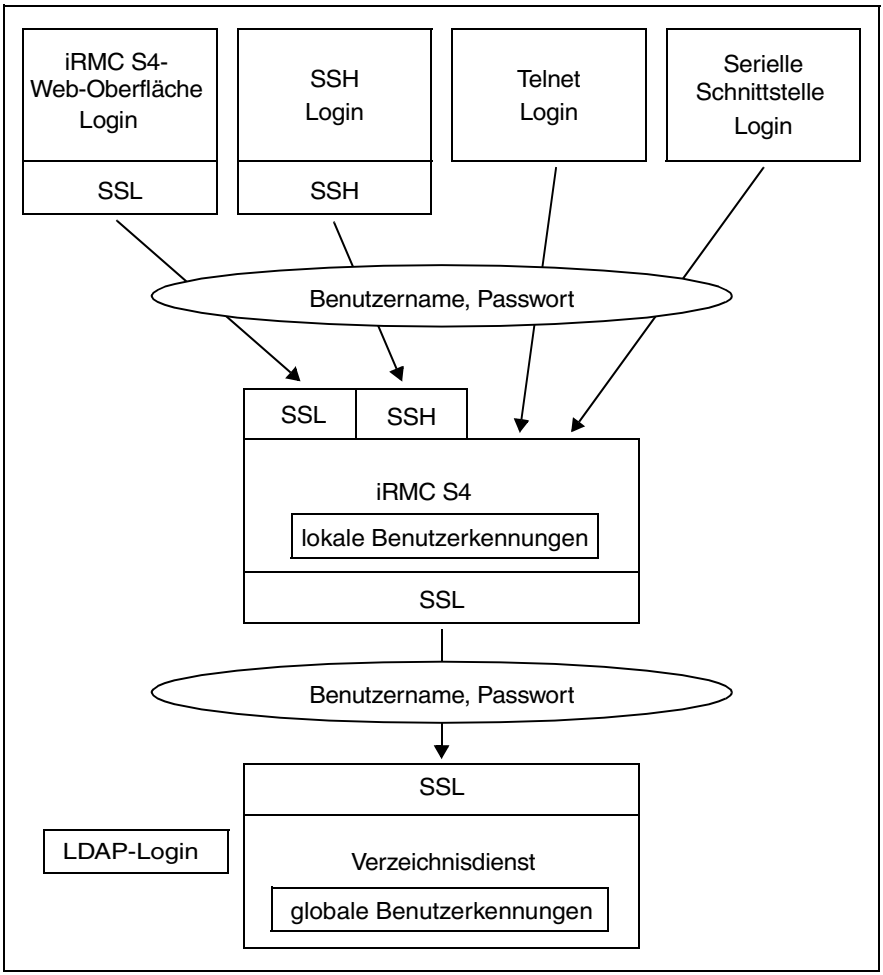


Bild 59: Login-Authentifizierung durch den iRMC S4

Die Nutzung von SSL für die LDAP-Verbindung zwischen dem iRMC S4 und dem Verzeichnisdienst ist optional, wird jedoch empfohlen. Eine SSL-gesicherte LDAP-Verbindung zwischen iRMC S4 und Verzeichnisdienst garantiert den sicheren Austausch der Daten, insbesondere auch von Benutzernamen und Passwort.

SSL-Login über die iRMC S4-Web-Oberfläche ist nur dann erforderlich, wenn LDAP aktiviert ist (siehe Handbuch "iRMC S4 integrated Remote Management Controller").

8.2 Globale Benutzerverwaltung für den iRMC S4

Die globalen Benutzerkennungen für den iRMC S4 werden zentral für alle Plattformen mithilfe eines LDAP-Verzeichnisdienstes verwaltet.

Für die iRMC S4-Benutzerverwaltung werden zurzeit folgende Verzeichnisdienste unterstützt:

- Microsoft® Active Directory
- Novell® eDirectory
- OpenLDAP
- Open DS / ForgeRock's OpenDJ

Dieser Abschnitt informiert über folgende Themen:

- Überblick über die globale Benutzerverwaltung für den iRMC S4
- Konzept der globalen Benutzerverwaltung für den iRMC S4 mithilfe eines LDAP-Verzeichnisdienstes
- Globale iRMC S4-Benutzerverwaltung im Verzeichnisdienst konfigurieren (iRMC S4-spezifische Berechtigungsstrukturen im Verzeichnisdienst generieren).
- Globale iRMC S4-Benutzerverwaltung via Microsoft Active Directory
- Globale iRMC S4-Benutzerverwaltung via Novell eDirectory
- Globale iRMC S4-Benutzerverwaltung via OpenLDAP/ OpenDS / OpenDJ

Neben den in diesem Abschnitt beschriebenen Maßnahmen, die Sie auf Seiten des Verzeichnisdienstes durchführen, erfordert die globale Benutzerverwaltung außerdem die Konfiguration der lokalen LDAP-Einstellungen am iRMC S4.

Die lokalen LDAP-Einstellungen konfigurieren Sie wahlweise (siehe Handbuch "iRMC S4 - integrated Remote Management Controller"):

- an der iRMC S4-Web-Oberfläche,
- mithilfe des Server Configuration Managers.

Die Konfiguration der Einstellungen für die globale iRMC S4-Benutzerverwaltung erfordert detaillierte Kenntnisse des verwendeten Verzeichnisdienstes. Nur Personen mit den entsprechenden Kenntnissen sollten die Konfiguration durchführen.

8.2.1 Überblick

Die globalen Benutzerkennungen für den iRMC S4 werden zentral und Plattform-übergreifend im Verzeichnis (Directory) eines Verzeichnisdienstes abgelegt. Auf diese Weise lassen sich die Benutzerkennungen auf einem zentralen Server verwalten und können somit von allen iRMC und iRMC S4 verwendet werden, die mit diesem Server im Netz verbunden sind.

Der Einsatz eines Verzeichnisdienstes für den iRMC S4 ermöglicht es darüber hinaus, für das Anmelden an den iRMC S4 dieselben Benutzerkennungen zu verwenden wie für das Anmelden am Betriebssystem der verwalteten Server.

Für die folgenden iRMC S4-Funktionen wird zurzeit die globale Benutzerverwaltung nicht unterstützt:

- Login via IPMI-over-LAN
- Text-Konsolen-Umleitung via SOL

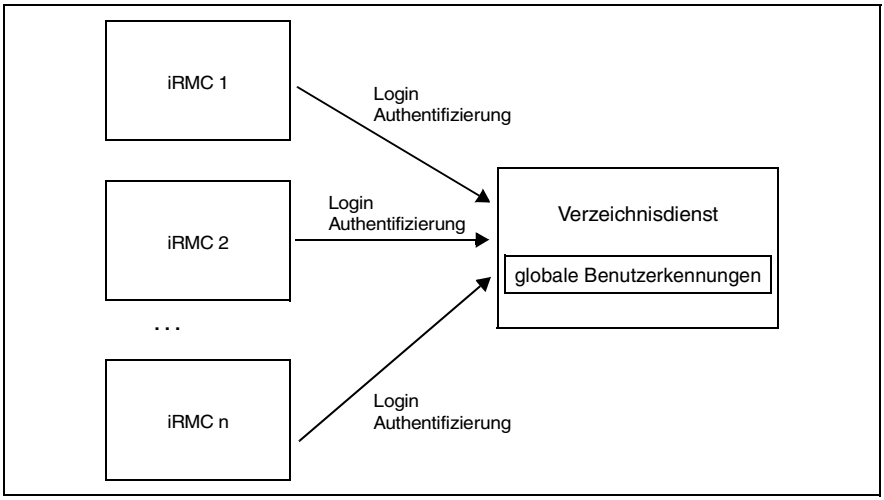


Bild 60: Gemeinsame Nutzung der globalen Benutzerkennungen durch mehrere iRMC S4

Die Kommunikation zwischen den einzelnen iRMC S4 und dem zentralen Verzeichnisdienst wird über das TCP/IP-Protokoll LDAP (**L**ightweight **D**irectory **A**ccess **P**rotocol) abgewickelt. LDAP ermöglicht den Zugriff auf die gängigsten zur Benutzerverwaltung geeigneten Verzeichnisdienste. Die Kommunikation über LDAP kann optional durch SSL abgesichert werden.

8.2.2 iRMC S4-Benutzerverwaltung mithilfe eines LDAP-Verzeichnisdienstes (Konzept)

Das im Folgenden erläuterte Konzept einer Verzeichnisdienst-gestützten, globalen iRMC S4-Benutzerverwaltung gilt gleichermaßen für die Verzeichnisdienste Microsoft Active Directory, Novell eDirectory, OpenLDAP und OpenDS / OpenDJ. Die Abbildungen zeigen exemplarisch die Konsole *Active Directory-Benutzer und -Computer* der Benutzeroberfläche von Microsoft Active Directory.

Die folgenden Zeichen sind in LDAP als Meta-Zeichen für Such-Strings reserviert: *, \, &, (,), |, !, =, <, >, ~, :

Verwenden Sie diese Zeichen deshalb nicht als Bestandteil von Relative Distinguished Names (RDN).

8.2.2.1 Globale iRMC S4-Benutzerverwaltung über Berechtigungsgruppen und Rollen

Die globale iRMC S4-Benutzerverwaltung mithilfe eines LDAP-Verzeichnisservers (LDAP Directory Server) erfordert keine Erweiterung des Standard-Schemas des Verzeichnisservers. Vielmehr werden sämtliche für den iRMC S4 relevanten Informationen einschließlich der Benutzerberechtigungen (Privilegien) über zusätzliche LDAP-Gruppen und Organisationseinheiten (Organizational Units, OU) bereitgestellt, die in einer separaten OU innerhalb einer Domäne des LDAP-Verzeichnisservers in separaten OUs zusammengefasst sind (siehe Bild 62 auf Seite 237).

iRMC S4-Benutzer erhalten ihre Privilegien über die Zuweisung einer in der Organizational Unit (OU) *SVS* deklarierten Rolle (Benutzerrolle).

Rechtevergabe über Benutzerrollen (kurz: Rollen, Role)

Die globalen Benutzerverwaltung am iRMC S4 (Firmware-Version 3.77 oder höher) regelt die Rechtevergabe über Benutzerrollen. Dabei definiert jede Rolle ein spezifisches, aufgabenorientiertes Berechtigungsprofil für Tätigkeiten am iRMC S4.

Jedem Benutzer können mehrere Rollen zugewiesen werden, sodass sich die Rechte dieses Benutzers aus der Gesamtheit der Rechte aller zugewiesenen Rollen ableiten.

Bild 61 skizziert das Konzept der rollenbasierten Vergabe von Benutzerberechtingungen mit den Rollen *Administrator*, *Maintenance*, *Observer* und *UserKVM*.

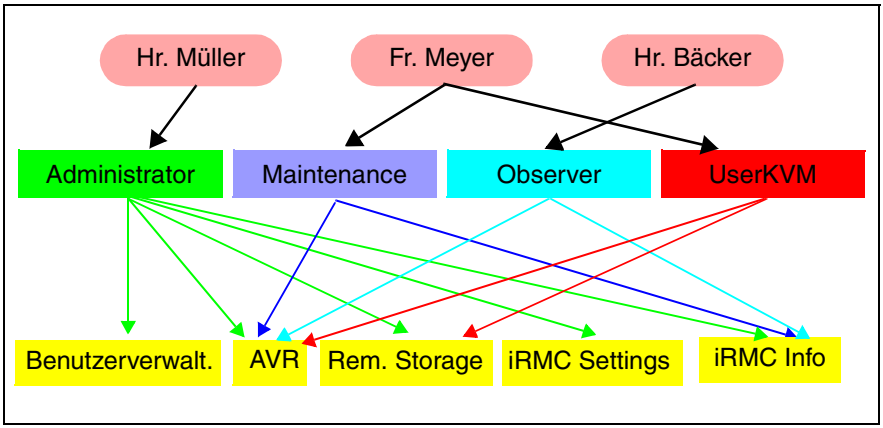


Bild 61: Rollenbasierten Vergabe von Benutzerberechtigungen

Das Konzept der Benutzerrollen bietet u.a folgende wesentlichen Vorteile:

– Die einzelnen Berechtigungen müssen nicht jedem Benutzer oder jeder Benutzergruppe separat zugewiesen werden, sondern nur der Benutzerrolle.

– Wenn sich die Berechtigungsstruktur ändert, müssen nur die Rechte der Benutzerrolle angepasst werden.

8.2.2.2 Organizational Unit (OU) SVS

Die Firmware des iRMC S2 ab Firmware-Version 3,77A und des iRMC S3 unterstützen LDAP v2-Strukturen, die in der OU *SVS* abgelegt sind. LDAP v2-Strukturen sind für künftige funktionale Erweiterungen ausgelegt.

SVS enthält die OUs *Declarations*, *Departments* und *User Settings*:

– *Declarations* enthält eine Liste der definierten Rollen sowie die Liste der vordefinierten iRMC S4-Benutzerberechtigungen (siehe Handbuch "iRMC S4 - integrated Remote Management Controller").

– *Departments* enthält die Gruppen für die Benutzerprivilegien.

– *User Settings* enthält Benutzer(gruppen)-spezifische Angaben, wie z.B. das Mail-Format (für die E-Mail-Benachrichtigung) und die Gruppen für die Benutzershells.

Bei Microsoft Active Directory z.B. können die Einträge für die iRMC S4-Benutzer in der Standard OU *Users* liegen. Im Gegensatz zu den Standardbenutzern sind iRMC S4-Benutzer jedoch zusätzlich Mitglied in einer oder mehreren Gruppen der OU *SVS*.

Wichtiger Hinweis:

Die Abwicklung sowohl der ServerView- als auch des iRMC S4-Benutzerverwaltung innerhalb derselben Organizational Unit (OU) SVS setzt voraus, dass der iRMC S4 als Element des Departments DEFAULT konfiguriert ist.

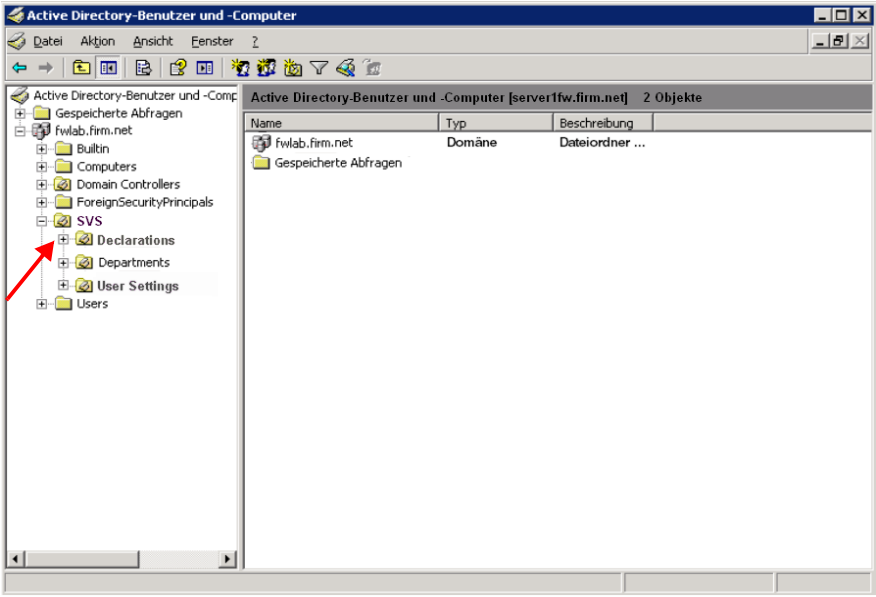


Bild 62: OU SVS in der Domäne fwlab.firm.net

Die Benutzereinträge für den iRMC S4 können ab der Firmware-Version 3.6x an beliebigen Stellen unterhalb der Basis-Domäne liegen. Ebenso können Berechtigungsgruppen an beliebigen Stellen innerhalb der Basisdomäne liegen.

8.2.2.3 Server-übergreifende globale Benutzerberechtigungen

In größeren Unternehmen sind die via iRMC S4 verwalteten Server in der Regel verschiedenen Abteilungen zugeordnet. Außerdem werden die Administrator-Berechtigungen für die verwalteten Server ebenfalls oft abteilungsspezifisch vergeben.

Wichtiger Hinweis:

Die Abwicklung sowohl der ServerView- als auch der iRMC S4-Benutzerverwaltung innerhalb derselben Organizational Unit (OU) SVS setzt voraus, dass der iRMC S4 als Element des Departments DEFAULT konfiguriert ist.

Abteilungen sind in der OU „Departments“ zusammengefasst

Die OU *Departments* fasst die via iRMC S4 verwalteten Server zu verschiedenen Gruppen zusammen. Diese entsprechen den Abteilungen, in denen jeweils dieselben Benutzerkennungen und -berechtigungen gelten. In Bild 63 auf Seite 239 z.B. sind dies die Abteilungen *DeptX*, *DeptY* und *Others*.

Der Eintrag *Others* ist optional, wird aber empfohlen. *Others* ist eine vordefinierte Abteilungsbezeichnung, unter der diejenigen Server zusammengefasst sind, die keiner anderen Abteilung angehören. Die Anzahl der unter *Departments* aufgelisteten Abteilungen (OUs) unterliegt keinen Einschränkungen.

Bei der Konfiguration des Verzeichnisdienstes am iRMC S4 über die iRMC S4-Web-Oberfläche oder über den Server Configuration Manager spezifizieren Sie den Namen der Abteilung, welcher der verwaltete Server mit dem betreffenden iRMC S4 angehört. Existiert im LDAP-Verzeichnis keine Abteilung dieses Namens, dann werden die Berechtigungen der Abteilung *Others* verwendet.

Bild 63 auf Seite 239 zeigt anhand von *Active Directory-Benutzer und -Computer* ein Beispiel für eine solche Organisationsstruktur.

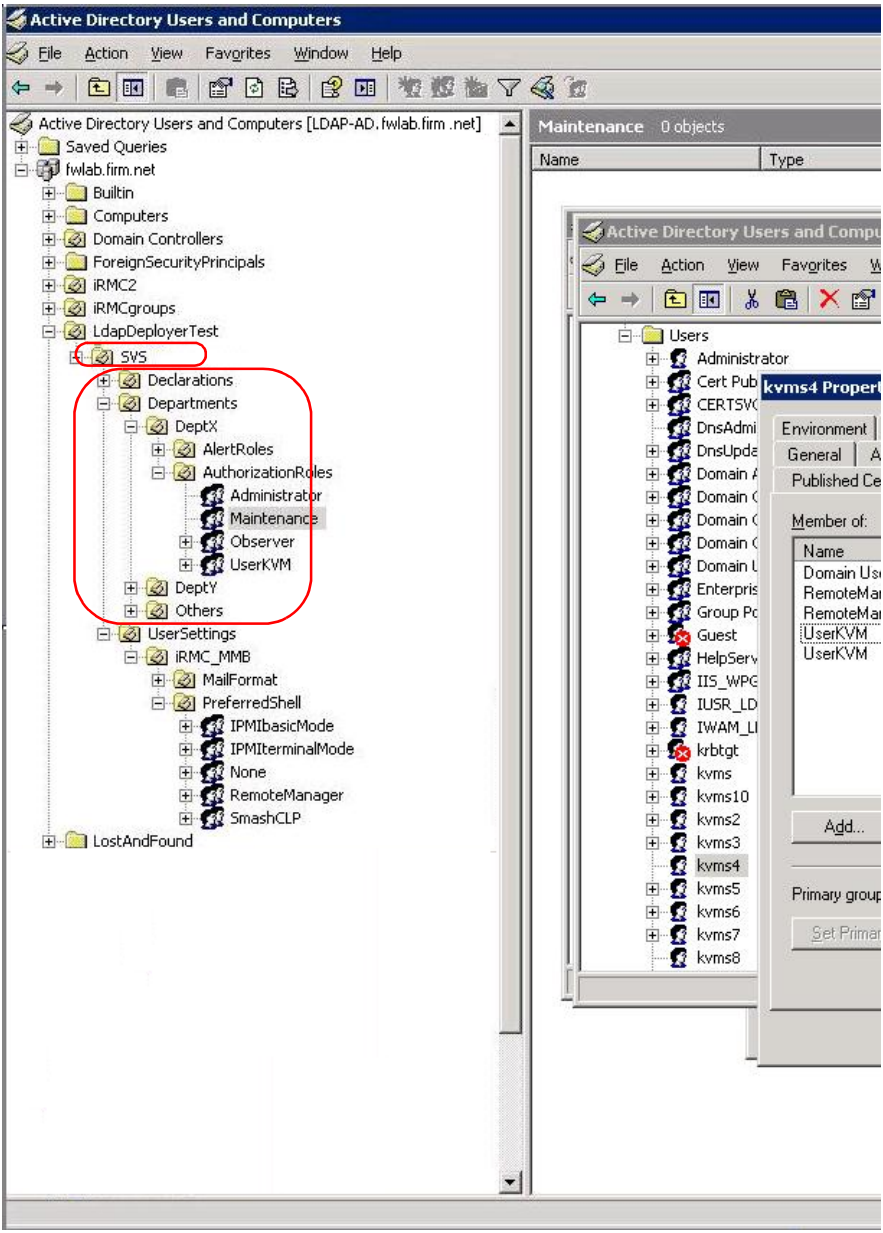


Bild 63: Organistionsstruktur der Domäne fwlab.firm.net

8.2.2.4 SVS: Berechtigungsprofile werden über Rollen definiert

Direkt unterhalb jeder Abteilung sind die gewünschten zugehörigen Benutzerrollen (Authorization Roles) aufgeführt (Bild 63 auf Seite 239). Alle hier aufgeführten Rollen müssen in der OU *Declarations* definiert sein. Ansonsten gibt es hinsichtlich Anzahl der Roles keine Einschränkungen. Die Namen der Rollen sind unter Beachtung einiger syntaktischer Vorgaben des verwendeten Verzeichnisdienstes frei wählbar. Jede Authorization Role definiert ein spezifisches, aufgabenorientiertes Berechtigungsprofil für Tätigkeiten am iRMC S4.

Neben den Authorization Roles sind auch die Alert Roles aufgeführt. Jede Alert Role definiert ein spezifisches Benachrichtigungsprofil für die E-Mail-Benachrichtigung (siehe Abschnitt "E-Mail-Benachrichtigung an globale iRMC S4-Benutzer konfigurieren" auf Seite 299).

Benutzerrollen anzeigen

Wenn Sie im Strukturbaum von *Active Directory-Benutzer und -Computer* (siehe Bild 64) unter *SVS* eine Abteilung (z.B. *DeptX*) auswählen (1) und die zugehörigen Knoten *DeptX – Authorization Roles* aufklappen, werden die Benutzerrollen angezeigt (2), die für diese Abteilung (hier: *DeptX*) definiert sind.

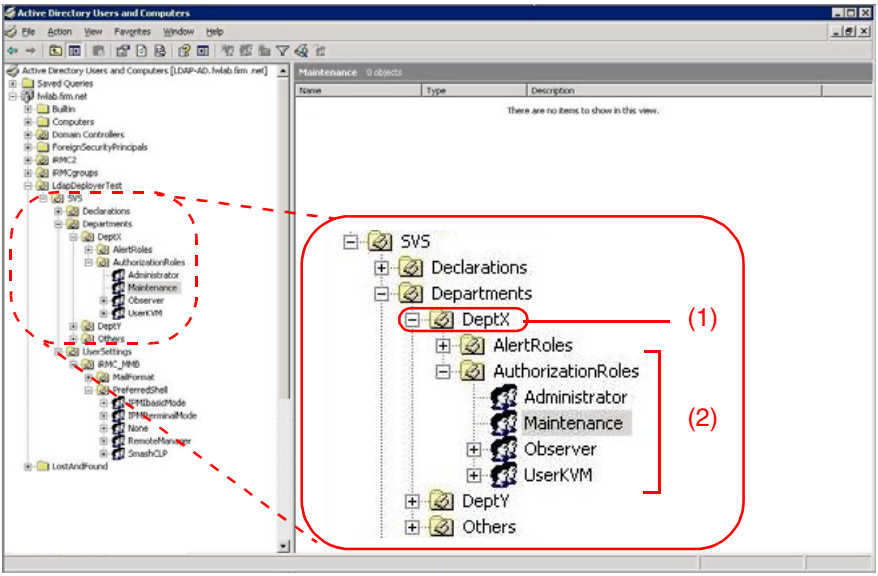


Bild 64: Anzeige der Benutzerrollen im Snap-in „Benutzer und -Computer

Berechtigungsgruppen anzeigen, denen ein Benutzer zugeordnet ist

Wenn Sie im Strukturbaum von *Active Directory Users and Computers*(siehe Bild 65) unter *Benutzer* einen Benutzer (z.B. *kvms4*) auswählen (1) und via Kontextmenü *Eigenschaften – Mitglieder* den *Eigenschaften*-Dialog für diesen Benutzer öffnen, werden in der Registerkarte *Mitglieder* die Berechtigungsgruppen angezeigt (2), denen der Benutzer (hier: *kvms4*) angehört.

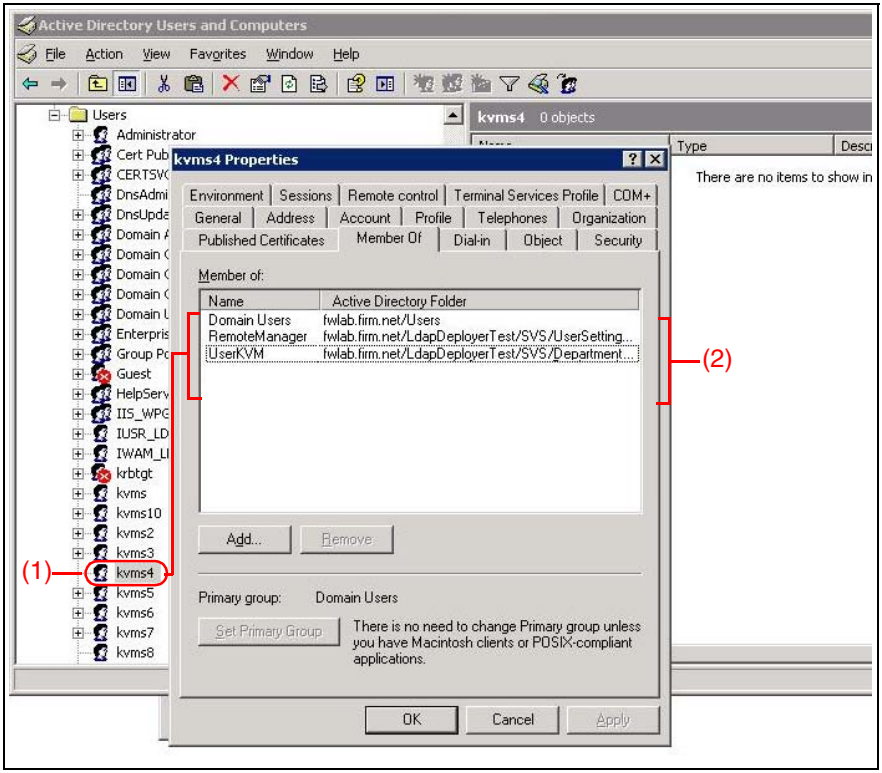


Bild 65: Eigenschaften-Dialog des Benutzers kvms4

8.2.3 SVS_LdapDeployer - Struktur „SVS“ generieren, pflegen und löschen

Um die globale iRMC S4-Benutzerverwaltung über einen Verzeichnisdienst abwickeln zu können, müssen im LDAP-Verzeichnisdienst die Struktur (OU) *SVS* .

Zum Generieren sowie zum Anpassen von *SVS*-Strukturen verwenden Sie den *SVS_LdapDeployer*. Der *SVS_LdapDeployer* ist ein Java-Archiv (*SVS_LdapDeployer.jar*), das Sie im Firmware-Package auf Ihrer ServerView Suite DVD finden.

Dieser Abschnitt beschreibt:

– Konfigurationsdatei des *SVS_LdapDeployer*

– *SVS_LdapDeployer*

– Kommandos und Optionen des *SVS_LdapDeployer*

– Typische Anwendungsszenarien

8.2.3.1 Konfigurationsdatei (xml-Datei)

SVS_LdapDeployer erzeugt LDAP-Strukturen auf Basis einer *xml*-Konfigurationsdatei. Diese Eingabedatei enthält die Strukturinformationen für die Struktur *SVS* in xml-Syntax.

Die Syntax der Konfigurationsdatei ersehen Sie aus den Beispiel-Konfigurationsdateien *Generic_Settings.xml* und *Generic_InitialDeploy.xml*, die Sie zusammen mit dem *jar*-Archiv *SVS_LdapDeployer.jar* auf der ServerView Suite DVD ausgeliefert werden.

In der Eingabedatei müssen unter <Settings> immer gültige Verbindungsdaten für die Verbindung zum Verzeichnisserver eingetragen sein.

Optional können Sie auch die Authentisierungsdaten für den Server-Zugriff eintragen. Alternativ können Sie die Authentisierungsdaten auch in der Kommandozeile des *SVS_LdapDeloyer* angeben.

Wenn Sie die Authentisierungsdaten weder in der Konfigurationsdatei noch in der Kommandozeile beim Aufruf des *SVS_LdapDeployer* angeben, fordert der *SVS_LdapDeployer* die Authentisierungsdaten zum Ausführungszeitpunkt an.

8.2.3.2 SVS_LdapDeployer starten

Zum Starten des *SVS_LdapDeployer* gehen Sie wie folgt vor:

- Speichern Sie das Java-Archiv (*jar*-Archiv) *SVS_LdapDeployer.jar* in ein Verzeichnis auf dem Verzeichnisserver.
- Öffnen Sie die Kommando-Schnittstelle des Verzeichnisservers.
- Wechseln Sie in das Verzeichnis, in dem das *jar*-Archiv *SVS_LdapDeployer.jar* gespeichert ist.
- Rufen Sie den *SVS_LdapDeployer* gemäß dem folgenden Syntax-Schema auf:

```
java –jar SVS_LdapDeployer.jar <kommando> <datei>
                                                [<option>...]
```

Während der Ausführung des *SVS_LdapDeployer* werden Sie über die durchgeführten Schritte informiert. Detaillierte Informationen finden Sie in der Datei *log.txt*, die bei jeder Ausführung des *SVS_LdapDeployer* im Ausführungsverzeichnis angelegt wird.

Im Folgenden werden die Begriffe "LDAPv1-Struktur" und "LDAPv2-Struktur" für die Bezeichnung ServerView-spezifischer Konfigurationslayouts der Autorisierungsdaten verwendet und beziehen sich nicht auf die Versionen 1 und 2 des LDAP-Protokolls.

Die Kommandos *-import* und *-sychronize* (siehe unten) werden nur in Verbindung mit LDAPv1-Strukturen benötigt (iRMC S2s mit einer Firmware-Version < 3.77 und iRMCs). Näheres hierzu finden Sie in den Handbüchern

- "iRMC S2 - integrated Remote Management Controller", Ausgabe Mai 2011 und frühere Ausgaben.
- "iRMC - integrated Remote Management Controller"

<kommando>

Spezifiziert die durchzuführende Aktion.

Folgende Kommandos stehen zur Auswahl:

-deploy

Erzeugt auf dem Verzeichnisserver eine LDAP-Struktur für die globale iRMC S4-Benutzerverwaltung (siehe Seite 245).

-delete
: Löscht auf dem Verzeichnisserver eine vorhandenen LDAP-Struktur, die für die globale iRMC / iRMC S4-Benutzerverwaltung verwendet wird (siehe Seite 247).

-import
: Erzeugt aus einer existierenden LADAP v1-Struktur eine äquivalente LDAP v2-Struktur (siehe Seite 245).

-synchronize
: Zieht Änderungen, die Sie in einer LDAP v2-Struktur vornehmen, in einer bereits vorhandenen LDAP v1-Struktur nach (siehe Seite 245).

<datei>
: Konfigurationsdatei (*.xml*), die von *SVS_LdapDeploy* als Eingabedatei verwendet wird. Die Konfigurationsdatei enthält die Strukturinformationen für die Struktur(en) *SVS* in *xml*-Syntax.

Die Syntax der Konfigurationsdatei ersehen Sie aus den Beispiel-Konfigurationsdateien *Generic_Settings.xml* und *Generic_InitialDeploy.xml*, die zusammen mit dem *jar*-Archiv *SVS_LdapDeployer.jar* auf der ServerView Suite DVD ausgeliefert wird.

<option> [<option> ...]
: Option(en), die die Ausführung des spezifizierten Kommandos steuern.

In den nachfolgenden Abschnitten werden die einzelnen Kommandos des *SVS_LdapDeployer* samt den zugehörigen Optionen im Detail erläutert.

Der *SVS_LdapDeployer* erzeugt alle benötigten Unterbäume inklusive aller Gruppen, nicht jedoch die Beziehungen zwischen Benutzern und Gruppen.

Die Erstellung und Zuordnung von Benutzereinträgen zu Gruppen nehmen Sie über ein entsprechendes Tool des verwendeten Verzeichnisdienstes vor, nachdem Sie die OU *SVS* im Verzeichnisdienst generiert haben.

8.2.3.3 -deploy: LDAP-Struktur erzeugen oder ändern

Mit dem Kommando *-deploy* können Sie auf dem Verzeichnisserver eine neue LDAP-Struktur erzeugen oder zu einer bereits existierende LDAP-Struktur neue Einträge hinzufügen.

Zum Entfernen von Einträgen aus einer existierenden LDAP-Struktur, müssen Sie die LDAP-Struktur zuerst mit *-delete* löschen (siehe Seite 247) löschen und anschließend mit einer entsprechend modifizierten Konfigurationsdatei neu generieren.

Syntax:

```
-deploy <datei> [-structure {v1 | v2 | both}]
      [ -username <benutzer>]
      [ -password <passwort>][ -store_pwd <pfad>][ -kloc <pfad>]
      [ -kpwd [<key-passwort>]]
```

<datei>

xml-Datei, die die Konfigurationsdaten enthält.

Die Konfigurationsdatei muss unter <Data> alle erforderlichen Rollen und Abteilungen enthalten, die für das erstmalige Generieren bzw. die Erweiterung einer Struktur benötigt werden.

-structure v1 | -structure v2 | -structure both

Erzeugt eine LDAP v1-Struktur oder eine LDAP v2-Struktur oder eine LDAP v1- und eine LDAP v2-Struktur.

-username <benutzer>

Benutzername zur Anmeldung am Verzeichnisserver.

-password <passwort>

Passwort für den Benutzer <benutzer>

-store_pwd

Verschlüsselt das Passwort <passwort> mithilfe eines zufallsgenerierten Schlüssels und speichert das verschlüsselte Passwort nach erfolgreicher Ausführung von *-deploy* in der Konfigurationsdatei ab. Der zufallsgenerierte Schlüssel wird standardmäßig in dem Ordner abgespeichert, in dem der *SVS_LdapDeployer* ausgeführt wird.

ACHTUNG!

Den zufallsgenerierten Schlüssel sollten Sie sicher abspeichern. Falls der voreingestellte Zielordner Ihren Sicherheitserfordernissen nicht genügt oder der Ordner, in dem der Schlüssel gespeichert wird, auch anderen Benutzern zugänglich ist, verwenden Sie für eine sichere Speicherung des Schlüssels die Optionen *-kloc* und *-kpwd*.

-kloc <pfad>

Speichert den zufallsgenerierten Schlüssel unter <pfad>.
Wenn Sie diese Option nicht angeben, wird der Schlüssel im dem Ordner gespeichert, in dem der *SVS_LdapDeployer* ausgeführt wird.

-kpwd [<passwort>]

Legt ein Passwort zum Schutz des zufallsgenerierten Schlüssels fest.
Wenn Sie <passwort> nicht angeben, wird das Passwort automatisch auf Basis einer Momentaufnahme der aktuellen Ablaufumgebung gebildet.

8.2.3.4 -delete: LDAP-Struktur löschen

Mit dem Kommando *-delete* können Sie auf dem Verzeichnisserver eine LDAP-Struktur entfernen.

Syntax:

```
-delete <datei> [-structure {v1 | v2 | both}]
      [ -username <benutzer>]
      [ -password <passwort>][ -store_pwd <pfad>][ -kloc <pfad>]
      [ -kpwd [<key-passwort>]]
```

<datei>
xml-Datei, die die zu löschende Struktur spezifiziert.

-structure v1 | -structure v2 | -structure both
Löscht LDAP v1-Struktur oder LDAP v2-Struktur oder LDAP v1- und LDAP v2-Struktur.

-username <benutzer>
Benutzername zur Anmeldung am Verzeichnisserver

-password <passwort>
Passwort für den Benutzer <benutzer>

-stor_pwd
Verschlüsselt das Passwort <passwort> mithilfe eines zufallsgenerierten Schlüssels und speichert das verschlüsselte Passwort nach erfolgreicher Ausführung von *-delete* in der Konfigurationsdatei ab. Der zufallsgenerierte Schlüssel wird standardmäßig in dem Ordner abgespeichert, in dem der *SVS_LdapDeployer* ausgeführt wird.

ACHTUNG!

Den zufallsgenerierten Schlüssel sollten Sie sicher abspeichern. Falls der voreingestellte Zielordner Ihren Sicherheitserfordernissen nicht genügt oder der Ordner, in dem der Schlüssel gespeichert wird, auch anderen Benutzern zugänglich ist, verwenden Sie für eine sichere Speicherung des Schlüssels die Optionen *-kloc* und *-kpwd*.

-kloc <pfad>
Speichert den zufallsgenerierten Schlüssel unter <pfad>.
Wenn Sie diese Option nicht angeben, wird der Schlüssel im dem Ordner gespeichert, in dem der *SVS_LdapDeployer* ausgeführt wird.

-kpwd [<passwort>]
Legt ein Passwort zum Schutz des zufallsgenerierten Schlüssels fest. Wenn Sie <passwort> nicht angeben, wird das Passwort automatisch auf Basis einer Momentaufnahme der aktuellen Ablaufumgebung gebildet.

8.2.4 Typische Anwendungsszenarien

Im Folgenden sind vier typische Szenarien für den Einsatz des *SVS_LdapDeployer* beschrieben.

8.2.4.1 Erst-Konfiguration einer LDAP v2-Struktur durchführen

Sie wollen erstmals die globale Benutzerverwaltung für einen iRMC S4 (Firmware-Version 3.77 oder höher) einrichten. Hierfür benötigen Sie eine LDAP v2-Struktur.

Empfohlene Vorgehensweise:

Generieren Sie eine Department-Definition für LDAP v2-Strukturen (*SVS*):

```
java -jar SVS_LdapDeployer.jar -deploy myInitialDeploy.xml
     -structure v2
```

8.2.4.2 LDAP v2-Struktur neu generieren oder erweitern

Sie wollen eine LDAP v2-Struktur neu generieren oder eine bereits bestehende LDAP v2-Struktur erweitern.

Empfohlene Vorgehensweise:

```
java -jar SVS_LdapDeployer.jar -deploy myInitialDeploy.xml
     -structure -structure v2
```

oder

```
java -jar SVS_LdapDeployer.jar -deploy myInitialDeploy.xml
```

8.2.4.3 LDAP v2-Struktur neu generieren und Authentisierungsdaten anfordern und speichern

Sie wollen eine LDAP v2-Struktur neu generieren. Die Authentisierungsdaten sollen via Kommandozeile bereitgestellt und gespeichert werden.

Empfohlene Vorgehensweise:

```
java –jar SVS_LdapDeployer.jar –deploy myInitialDeploy.xml
     –store_pwd –username admin –password admin
```

Nach dem Speichern der Anmeldedaten können Sie sich über den *SVS_LdapDeployer* ohne Angabe von Benutzerkennung und Passwort mit dem Verzeichnisserver verbinden. Der *SVS_LdapDeployer* verwendet dann - sofern vorhanden - die in der xml-Konfigurationsdatei gespeicherten Werte. Ein gespeichertes Passwort kann der *SVS_LdapDeployer* nur dann verwenden, wenn er es entschlüsseln kann. Dies erfordert, dass Sie den *SVS_LdapDeployer* in derselben Laufzeitumgebung aufrufen, wie beim vorangegangenen Aufruf mit *-store_pwd* (siehe Seite 246). „Dieselbe Laufzeitumgebung“ bedeutet hier „derselbe Benutzer am selben Computer“ oder „Benutzer mit Zugriffsberechtigung auf das Verzeichnis, unter dem der Schlüssel gespeichert ist (Option *-kloc*, siehe Seite 246)“.

Für zukünftige Aufrufe des *SVS_LdapDeployer* können Sie auch Benutzerkennungen verwenden, die bereits gespeichert sind. Darüber hinaus lassen sich durch explizite Angabe in der Kommandozeile oder auf Anforderung durch den *SVS_LdapDeployer* zeitweilig auch andere Authentisierungsdaten nutzen.

8.2.5 iRMC S4-Benutzerverwaltung via Microsoft Active Directory

Dieser Abschnitt beschreibt, wie Sie die iRMC S4-Benutzerverwaltung in Microsoft Active Directory integrieren.

Voraussetzung:

Eine LDAP v2-Struktur ist im Active Directory-Verzeichnisdienst generiert (siehe Abschnitt "SVS_LdapDeployer - Struktur „SVS“ generieren, pflegen und löschen" auf Seite 242).

Zur Integration der iRMC S4-Benutzerverwaltung in Microsoft Active Directory führen Sie die folgenden Schritte durch:

1. LDAP/SSL-Zugriff des iRMC S4 am Active Directory Server konfigurieren.
2. iRMC S4-Benutzer den iRMC S4-Benutzergruppen in Active Directory zuordnen.

8.2.5.1 LDAP/SSL-Zugriff des iRMC S4 am Active Directory Server konfigurieren

Die iRMC S4-LDAP-Integration verwendet die auf dem OpenSSL Project basierende SSL Implementation von Eric Young. Einen Abdruck des SSL Copyrights finden Sie auf Seite 307.

Die Nutzung von LDAP via SSL durch den iRMC S4 erfordert die Erstellung eines RSA-Zertifikats.

Die Konfiguration des LDAP-Zugriffs umfasst die folgenden Schritte:

1. Enterprise CA installieren.
2. RSA-Zertifikat für den Domänencontroller (Domain Controller) erzeugen.
3. RSA-Zertifikat auf dem Server installieren.

Enterprise CA installieren

Eine CA ist eine „Zertifizierungsstelle für Zertifikate“. Eine Enterprise CA („Zertifizierungsstelle für Unternehmen“) können Sie wahlweise auf dem Domänencontroller selbst oder auf einem anderen Server installieren.

Die Installation direkt auf dem Domänencontroller ist einfacher, da im Vergleich zur Installation auf einem anderen Server einige Installationsschritte entfallen.

Im Folgenden ist beschrieben, wie Sie die Enterprise CA direkt auf einem vom Domänencontroller verschiedenen Server installieren.

Die erfolgreiche Installation und Konfiguration einer Enterprise CA setzt eine Active Directory-Umgebung sowie die installierten IIS (**I**nternet **I**nformation **S**ervices) voraus.

Mit den folgenden Schritten installieren Sie eine Enterprise CA:

- Wählen Sie im Windows Startmenü:

  Start - Systemsteuerung - Software - Windows-Komponenten hinzufügen/entfernen

- Wählen Sie im Wizard für die Windows-Komponenten unter *Komponenten* den Punkt *Zertifikatsdienste*.
- Führen Sie einen Doppelklick auf *Zertifikatsdienste* aus und stellen Sie sicher, dass die Optionen *Webregistrierung für Zertifikatsdienste* und *Zertifizierungsstelle für Zertifikate* ausgewählt sind.
- Wählen Sie *Stammzertifizierungsstelle eines Unternehmens*.

- ► Aktivieren Sie die Option *Schlüsselpaar und Zertifizierungsstellenzertifikat mit diesen Einstellungen erstellen*.
- ► Wählen Sie *Microsoft Base DSS Cryptographic Provider*, um DSA-Zertifikate mit einer Schlüssellänge von 1024 Byte zu generieren.
- ► Exportieren Sie das öffentliche Zertifizierungsstellenzertifikat (CA Certificate).

  Im Einzelnen verfahren Sie hierfür wie folgt:

  - ► Starten Sie die Management-Konsole durch Eingabe von *mmc* in der Windows Eingabeaufforderung.
  - ► Fügen Sie das Snap-in für Zertifikate des lokalen Computers hinzu.
  - ► Navigieren Sie zu *Zertifikate (Lokaler Computer) - Vertrauenswürdige Stammzertifizierungsstellen - Zertifikate* und führen Sie einen Doppelklick aus.
  - ► Führen Sie einen Doppelklick auf das Zertifikat der neu erstellten Zertifizierungsstelle aus.
  - ► Klicken Sie im Zertifikatsfenster auf die Registerkarte *Details*.
  - ► Klicken Sie auf *In Datei kopieren*.
  - ► Wählen Sie einen Dateinamen für das Zertifizierungsstellenzertifikat und klicken Sie auf *Fertig stellen*.
- ► Laden Sie das öffentliche Zertifizierungsstellenzertifikat auf dem Domänencontroller in das Zertifikatsverzeichnis *Vertrauenswürdige Stammzertifizierungsstellen*.

  Im Einzelnen verfahren Sie hierfür wie folgt:

  - ► Übertragen Sie die Datei des Zertifizierungsstellenzertifikats auf den Domänencontroller.
  - ► Öffnen Sie im Windows Explorer das Zertifikat der neu erstellten Zertifizierungsstelle.
  - ► Klicken Sie auf *Zertifikat installieren*.
  - ► Klicken Sie unter *Alle Zertifikate in folgenden Speicher speichern* auf *Durchsuchen* und wählen Sie *Vertrauenswürdige Stammzertifizierungsstellen*.
  - ► Starten Sie die Management-Konsole durch Eingabe von *mmc* in der Windows Eingabeaufforderung.

- ► Fügen Sie das Snap-in für Zertifikate des lokalen Computers hinzu.
- ► Fügen Sie das Snap-in für Zertifikate des aktuellen Benutzers hinzu.
- ► Kopieren Sie das Zertifizierungsstellenzertifikat (CA Certificate) aus dem Verzeichnis *Vertrauenswürdige Stammzertifizierungsstellen* des aktuellen Benutzers in das Verzeichnis *Vertrauenswürdige Stammzertifizierungsstellen* des lokalen Computers.

Domänencontroller-Zertifikat erzeugen

Mit den folgenden Schritten erstellen Sie ein RSA-Zertifikat für den Domänencontroller:

- ► Erstellen Sie eine Datei *request.inf* mit dem folgenden Inhalt:

```
[Version]
Signature="$Windows NT$"
[NewRequest]
Subject = "CN=<full path of domain controller host>"
KeySpec = 1
KeyLength = 1024
Exportable = TRUE
MachineKeySet = TRUE
SMIME = FALSE
PrivateKeyArchive = FALSE
UserProtected = FALSE
UseExistingKeySet = FALSE
ProviderName = "Microsoft RSA SChannel Cryptographic
Provider"
ProviderType = 12
RequestType = PKCS10
KeyUsage = 0xa0

[EnhancedKeyUsageExtension]
OID=1.3.6.1.5.5.7.3.1
; this is for Server Authentication
```

- ► Passen Sie in der Datei *request.inf* die Angaben bei „Subject=“ an den Namen des verwendeten Domänencontrollers an, z.B. `Subject = "CN=domino.fwlab.firm.net".`
- ► Geben Sie in der Windows Eingabeaufforderung folgendes Kommando ein: *certreq -new request.inf request.req*
- ► Geben Sie im Browser der Zertifizierungsstelle folgende URL ein: *http://localhost/certsrv*
- ► Klicken Sie auf *Ein Zertifikat anfordern.*

- ► Klicken Sie auf *erweiterte Zertifikatsanforderung.*
- ► Klicken Sie auf *Reichen Sie eine Zertifikatsanforderung ein.*
- ► Kopieren Sie den Inhalt der Datei *request.req* in das Fenster *Gespeicherte Anforderungen*.
- ► Wählen Sie die Zertifikatsvorlage *Webserver*.
- ► Laden Sie das Zertifikat herunter und speichern Sie es ab (z.B. in der Datei *request.cer*).
- ► Geben Sie in der Windows Eingabeaufforderung folgendes Kommando ein: *certreq -accept request.cer*
- ► Exportieren Sie das Zertifikat mit dem privaten Schlüssel.

  Im Einzelnen verfahren Sie hierfür wie folgt:

  - ► Starten Sie die Management-Konsole durch Eingabe vom *mmc* in der Windows Eingabeaufforderung.
  - ► Fügen Sie das Snap-in für Zertifikate des lokalen Computers hinzu.
  - ► Navigieren Sie zu *Zertifikate (Lokaler Computer) - Eigene Zertifikate - Zertifikate*.
  - ► Führen Sie einen Doppelklick auf das neue Server-Authentifizierungszertifikat aus.
  - ► Klicken Sie im Zertifikatsfenster auf die Registerkarte *Details*.
  - ► Klicken Sie auf *In Datei kopieren.*
  - ► Wählen Sie *Ja, privaten Schlüssel exportieren*.
  - ► Vergeben Sie ein Passwort.
  - ► Wählen Sie einen Dateinamen für das Zertifikat und klicken Sie auf *Fertig stellen*.

Domänencontroller-Zertifikat auf dem Server installieren

Mit den folgenden Schritten installieren Sie das Domänencontroller-Zertifikat auf dem Server:

- ► Kopieren Sie die soeben erstellte Datei für das Domänencontroller-Zertifikat auf den Domänencontroller.
- ► Führen Sie einen Doppelklick auf das Domänencontroller-Zertifikat aus.
- ► Klicken Sie auf *Zertifikat installieren.*
- ► Verwenden Sie das Passwort, das Sie beim Export der Zertifikats vergeben haben.
- ► Klicken Sie unter *Alle Zertifikate in folgendem Speicher speichern* auf die Schaltfläche *Durchsuchen* und wählen Sie *Eigene Zertifikate*.
- ► Starten Sie die Management-Konsole durch Eingabe von *mmc* in der Windows Eingabeaufforderung.
- ► Fügen Sie das Snap-in für Zertifikate des lokalen Computers hinzu.
- ► Fügen Sie das Snap-in für Zertifikate des aktuellen Benutzers hinzu.
- ► Kopieren Sie das Domänencontroller-Zertifikat aus dem Verzeichnis *Eigene Zertifikate* des aktuellen Benutzers in das Verzeichnis *Eigene Zertifikate* des lokalen Computers.

8.2.5.2 iRMC S4-Benutzer einer Rolle (Berechtigungsgruppe) zuordnen

Die Zuordnung von iRMC S4-Benutzern zu iRMC S4-Berechtigungsgruppen können Sie wahlweise vornehmen

– ausgehend vom Benutzereintrag oder
– ausgehend vom Rolleneintrag / Gruppeneintrag.

Nachfolgend ist am Beispiel der LDAP v2-Struktur die Zuordnung ausgehend vom Rolleneintrag anhand der OU *SVS* beschrieben.

Die Zuordnung ausgehend vom Benutzereintrag verläuft weitgehend analog.

In Active Directory müssen die Benutzer „von Hand“ in die Gruppen eingetragen werden.

Gehen Sie wie folgt vor:

► Öffnen Sie das Snap-in *Active Directory-Benutzer und -Computer*.

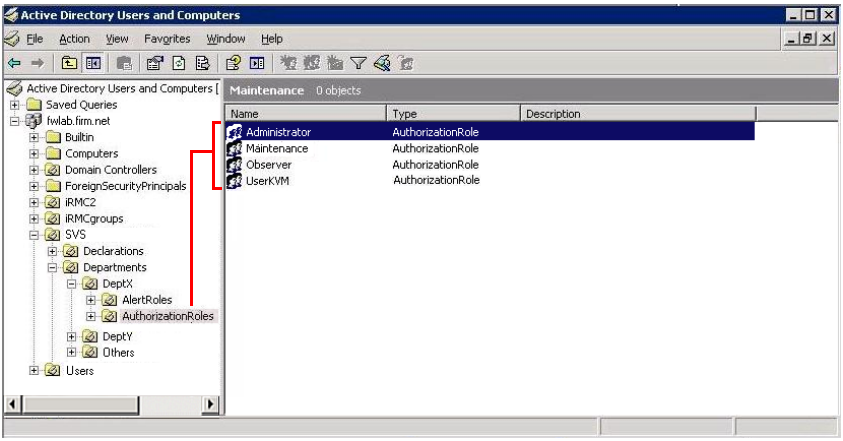


Bild 66: Snap-in Active Directory-Benutzer und -Computer

► Führen Sie einen Doppelklick auf die Berechtigungsgruppe (hier: Administrator) aus.

Der Dialog *Eigenschaften von Administrator* wird geöffnet (siehe Bild 67 auf Seite 257).

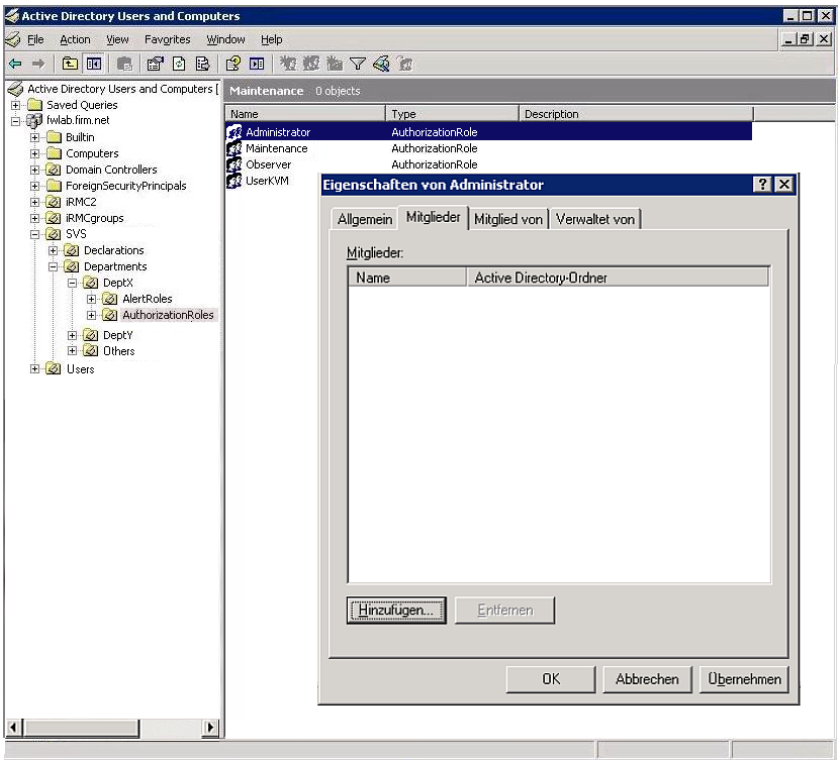


Bild 67: Dialog Eigenschaften von Administrator

- ► Wählen Sie die Registerkarte *Mitglieder*.
- ► Klicken Sie auf die Schaltfläche *Hinzufügen...* .

  Der Dialog *Benutzer, Kontakte oder Computer wählen* wird geöffnet (siehe Bild 68 auf Seite 258).

Bild 68: Dialog Benutzer, Kontakte oder Computer wählen

► Klicken Sie auf die Schaltfläche *Pfade...* .

Der Dialog *Pfad* wird geöffnet.

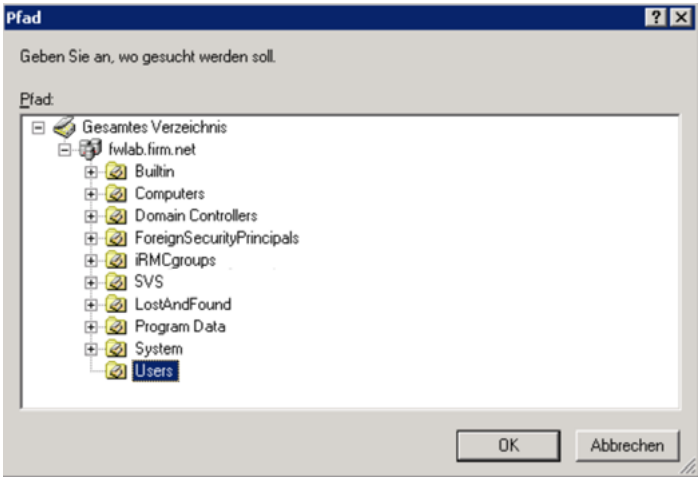


Bild 69: Dialog Pfad

► Wählen Sie den Container (OU), in dem sich Ihre Benutzer befinden. (Im Standardfall ist dies die OU *Users*.) Bestätigen Sie mit *OK*.

Der Dialog *Benutzer, Kontakte und Computer wählen* wird geöffnet (siehe Bild 70 auf Seite 259).

Benutzer können auch an anderer Stelle im Verzeichnis eingetragen sein.

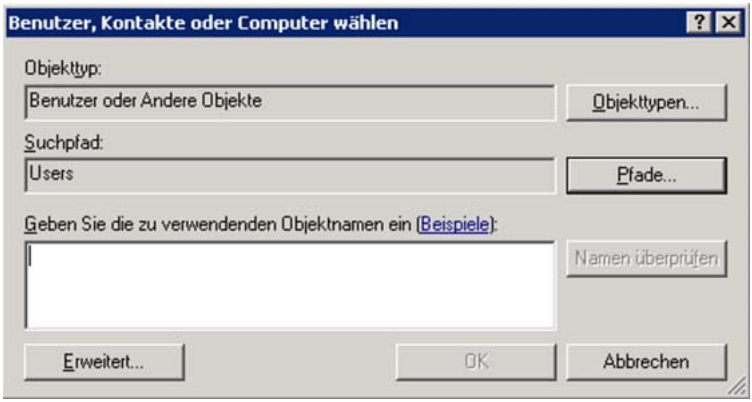


Bild 70: Dialog Benutzer, Kontakte oder Computer wählen

► Klicken Sie auf die Schaltfläche *Erweitert...* .

Ein erweiterter Dialog Benutzer, Kontakte und Computer wählen wird geöffnet (siehe Bild 71 auf Seite 260).

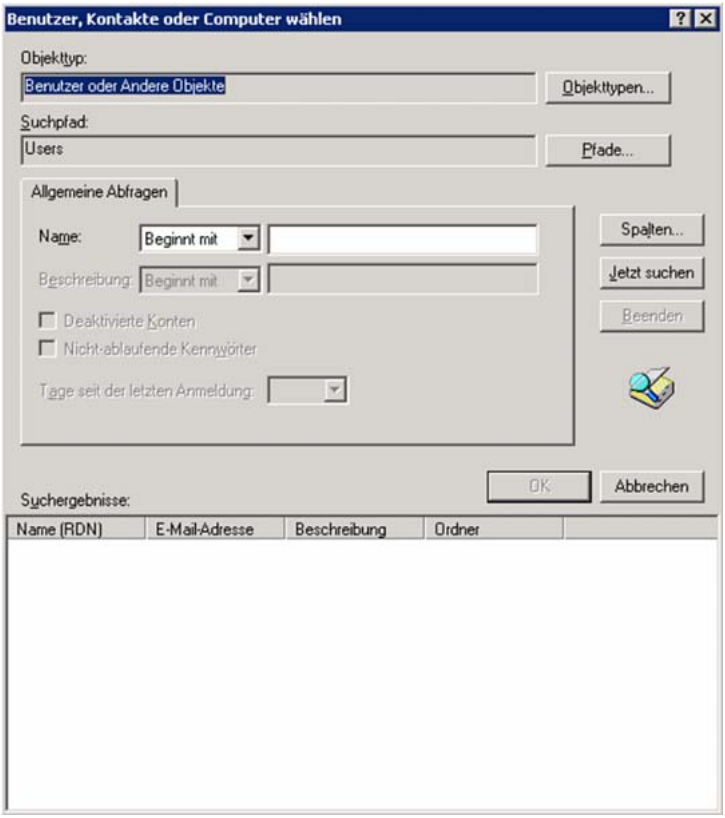


Bild 71: Dialog Benutzer, Kontakte oder Computer wählen - Suchen

- Klicken Sie auf die Schaltfläche *Jetzt suchen*, um sich alle Benutzer Ihrer Domäne anzeigen zu lassen.

  Im Anzeigebereich unter *Suchergebnisse:* wird das Suchergebnis angezeigt (siehe Bild 72 auf Seite 261).

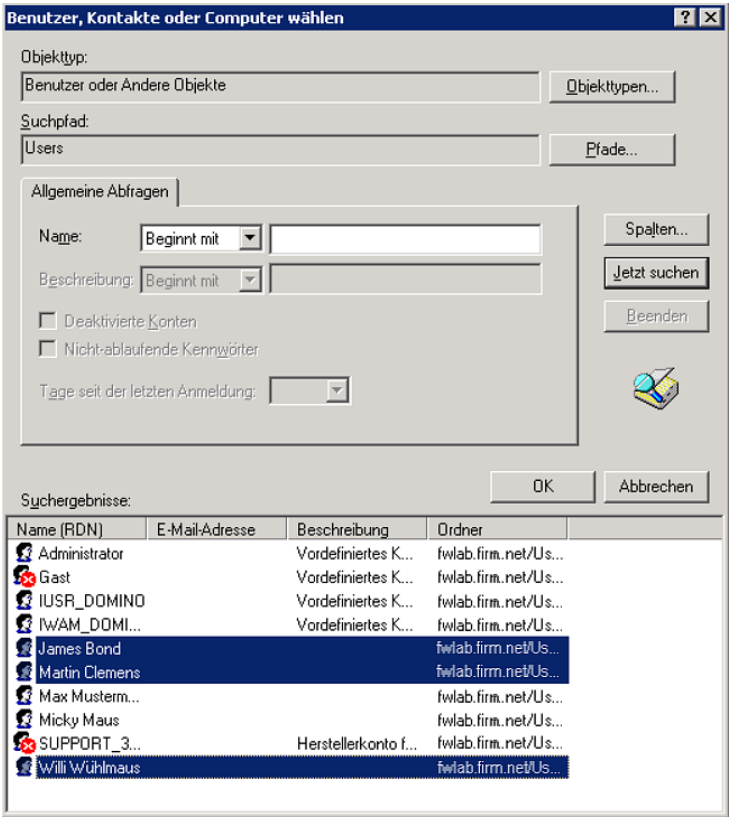


Bild 72: Dialog Benutzer, Kontakte oder Computer wählen - Suchergebnisse anzeigen

► Selektieren Sie die Benutzer, die zur Gruppe hinzugefügt werden sollen, und bestätigen Sie mit *OK*.

Es werden nun die ausgewählten Benutzer angezeigt (siehe Bild 73 auf Seite 262).

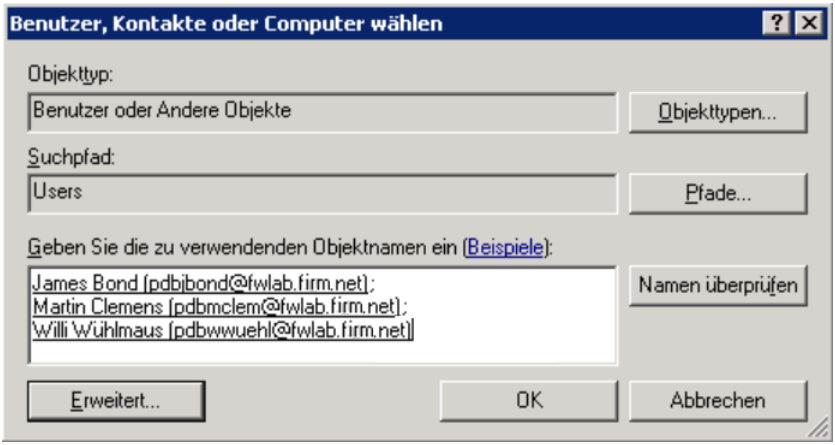


Bild 73: Dialog Benutzer, Kontakte oder Computer wählen - Suchergebnisse bestätigren

► Bestätigen Sie mit *OK*.

8.2.6 iRMC S4-Benutzerverwaltung via Novell eDirectory

Dieser Abschnitt informiert über die folgenden Themen:

– Software-Komponenten und Systemanforderungen von Novell eDirectory

– Novell eDirectory installieren.

– Novell eDirectory konfigurieren.

– iRMC S4-Benutzerverwaltung in Novell eDirectory integrieren.

– Tipps zur Administration von Novell eDirectory.

Installation und Konfiguration von Novell eDirectory werden im Folgenden ausführlich beschrieben. Tiefere eDirectory-Kenntnisse werden nicht vorausgesetzt. Sofern Sie bereits mit Novell eDirectory vertraut sind, können Sie die folgenden drei Abschnitte überspringen und fortfahren mit Abschnitt "iRMC S4-Benutzerverwaltung in Novell eDirectory integrieren" auf Seite 277.

8.2.6.1 Software-Komponenten und Systemanforderungen

Verwenden Sie jeweils die angegebene oder eine aktuellere Version der nachfolgend aufgelisteten Komponenten.

Novell eDirectory (ehemals NDS) besteht aus folgenden Software-Komponenten:

– eDirectory 8.8: *20060526_0800_Linux_88-SP1_FINAL.tar.gz*

– eDirectory 8.8: *eDir_88_iMan26_Plugins.npm*

– iManager: *iMan_26_linux_64.tgz* für SuSE, *iMan_26_linux_32.tgz* sonst

– ConsoleOne: *c1_136f-linux.tar.gz*

Für Installation und Betrieb von Novell eDirectory gelten die folgenden Systemanforderungen:

– OpenSSL muss installiert sein.

  Falls OpenSSL nicht bereits installiert ist:

  ► Installieren Sie OpenSSL, **bevor** Sie mit der Installation von Novell eDirectory beginnen.

– 512 MB freier Hauptspeicher

8.2.6.2 Novell eDirectory installieren

Die Installation von Novell eDirectory umfasst die Installation der folgenden Komponenten:

– eDirectory Server und Administrations-Utilities

– iManager (Administrations-Utility)

– ConsoleOne (Administrations-Utility)

Voraussetzung für die Installation von Novell eDirectory:

– Ein Linux Server-Betriebssystem muss komplett installiert sein und laufen.

– Die Firewall muss für Verbindungen zu folgenden Ports konfiguriert sein: 8080, 8443, 9009, 81, 389, 636.

  Für OpenSuSE konfigurieren Sie dies mithilfe der Datei */etc/sysconfig/SuSEfirewall2*:

  ► Erweitern Sie in der Datei */etc/sysconfig/SuSEfirewall2* den Eintrag *FW_SERVICES_EXT_TCP* wie folgt:

  ```
  FW_SERVICES_EXT_TCP="8080 8443 9009 81 389 636"
  ```

– Gemäß dem eDirectory Installation Guide muss das System für Multicast Routing eingerichtet sein.

  Für SuSE Linux gehen Sie hierfür wie folgt vor:

  ► Erzeugen oder (sofern bereits vorhanden) öffnen Sie die Datei */etc/sysconfig/network/ifroute-eth0*.

  ► Erweitern Sie */etc/sysconfig/network/ifroute-eth0* um die folgende Zeile:

  ```
  224.0.0.0  0.0.0.0  240.0.0.0  eth0
  ```

  Dadurch passen Sie *eth0* der Systemkonfiguration an.

Voraussetzungen für die Installation des eDirectory Servers, der eDirectory Utilities, des iManager und von ConsoleOne:

- Für die Installation ist Root-Berechtigung erforderlich.
- Die im Folgenden beschriebene Vorgehensweise bei der Installation setzt voraus, dass alle für die Installation benötigten Dateien bereits in ein Verzeichnis (z.B. */home/eDirectory*) kopiert wurden. Es handelt sich dabei um folgende Dateien:

  20060526_0800_Linux_88-SP1_FINAL.tar.gz
  iMan_26_linux_64.tgz
  c1_136f-linux.tar.gz

eDirectory Server und Administrations-Utilities installieren

Gehen Sie wie folgt vor:

- Melden Sie sich mit Root-Berechtigung (Super User) an.
- Wechseln Sie in das Verzeichnis, das die für die Installation benötigten Dateien enthält (im Beispiel: */home/eDirectory*):

  ```
  cd /home/eDirectory
  ```

- Extrahieren Sie das Archiv *20060526_0800_Linux_88-SP1_FINAL.tar.gz*:

  ```
  tar -xzvf 20060526_0800_Linux_88-SP1_FINAL.tar.gz
  ```

  Nach der Extraktion enthält */home/eDirectory* ein neues Unterverzeichnis *eDirectory*.

eDirectory Server installieren

- Wechseln Sie in das Unterverzeichnis *setup* dieses *eDirectory*-Verzeichnisses:

  ```
  cd eDirectory/setup
  ```

- Rufen Sie das Installationsskript *./nds-install* auf:

  ```
  ./nds-install
  ```

- Akzeptieren Sie die EULA mit „y“ und bestätigen Sie mit der Enter-Taste.
- Wenn Sie nach dem zu installierenden Programm gefragt werden:

  Geben Sie „1“ ein für die **Installation des Novell eDirectory Servers** und bestätigen Sie mit der Enter-Taste.

  Daraufhin werden die eDirectory-Packages installiert.

Nach der Installation des Novell eDirectory Servers müssen Sie in einigen Umgebungsvariablen die Namen für die Pfade auf das eDirectory aktualisieren und die Variablen exportieren.

- Öffnen Sie hierfür Ihre Konfigurationsdatei (im Beispiel: */etc/bash.bashrc*) und fügen Sie die dort vor „# End of ...“ die folgenden Zeilen in der angegebenen Reihenfolge ein:

```
export PATH/opt/novell/eDirectory/bin:/opt/novell/eDirectory/
       sbin:$PATH

export LD_LIBRARY_PATH=/opt/novell/eDirectory/lib:/
       opt/novell/eDirectory/lib/nds-modules:/opt/novell/
       lib:$LD_LIBRARY_PATH

export MANPATH=/opt/novell/man:/opt/novell/eDirectory/
       man:$MANPATH

export TEXTDOMAINDIR=/opt/novell/eDirectory/share/
       locale:$TEXTDOMAINDIR
```

- Schließen Sie das Terminal und öffnen Sie ein neues Terminal, um die Umgebungsvariablen zu exportieren.

eDirectory Administrations-Utilities installieren

- Wechseln Sie in das Unterverzeichnis *setup* des *eDirectory*-Verzeichnisses:

```
cd eDirectory/setup
```

- Rufen Sie das Installationsskript auf:

```
./nds-install
```

- Akzeptieren Sie die EULA mit „y“ und bestätigen Sie mit der Enter-Taste.
- Wenn Sie nach dem zu installierenden Programm gefragt werden:

  Geben Sie „2“ ein für die **Installation der Novell eDirectory Administrations-Utilities** und bestätigen Sie mit der Enter-Taste.

  Daraufhin werden die eDirectory Administrations-Utilities installiert.

iManager installieren und aufrufen

Der iManager ist das für die Administration von Novell eDirectory empfohlene Tool. Für die Installation sowohl in SLES10 als auch in OpenSuSE verwenden Sie das Archiv **_64.tgz*.

Gehen Sie wie folgt vor:

- Melden Sie sich mit Root-Berechtigung (Super User) an.
- Wechseln Sie in das Verzeichnis */home/eDirectory*:

  ```
  cd /home/eDirectory
  ```

- Extrahieren Sie das Archiv *iMan_26_linux_64.tgz*:

  ```
  tar -xzvf iMan_26_linux_64.tgz
  ```

  Nach der Extraktion enthält */home/eDirectory* ein neues Unterverzeichnis *iManager*.

- Wechseln Sie in das Unterverzeichnis *installs* von *iManager*:

  ```
  cd iManager/installs/linux
  ```

- Rufen Sie das Installationsskript auf:

  ```
  ./iManagerInstallLinux.bin
  ```

- Wählen Sie die Sprache, in der die Installationsmeldungen ausgegeben werden sollen.
- Klicken Sie durch die EULA und akzeptieren Sie die EULA.
- Wählen Sie *1- Novell iManager 2.6, Tomcat, JVM* zur iManager-Installation.
- Wählen Sie *1- Yes* für Plugin-Download.
- Klicken Sie auf Enter, um den Default-Pfad für den Download zu verwenden.

  Das Installationsprogramm sucht via Internet nach Downloads. Dies kann einige Minuten dauern. Danach werden Sie aufgefordert, die zu installierenden Plugins auszuwählen.

  - Wählen Sie *All* für den Download aller Plugins.
  - Wählen Sie *1- Yes* für die Installation der lokal verfügbaren Plugins.

- Drücken Sie auf Enter, um den Default-Pfad für die Installation zu verwenden.
- Wählen Sie *2- No* für die automatische Konfiguration von Apache (optional).

- Akzeptieren Sie den Default Port (8080) für Tomcat.
- Akzeptieren Sie den Default SSL-Port (8443) für Tomcat.
- Akzeptieren Sie den Default JK Connector-Port (9009) für Tomcat.
- Geben Sie die administrationsberechtigte Benutzerkennung (z.B. „root.fts“) für den administrationsberechtigten Benutzer ein.
- Geben Sie den Baumnamen (z.B. „fwlab“) für den administrationsberechtigten Benutzer ein.
- Akzeptieren die aufgelistete Zusammenfassung Ihrer Eingaben mit *1-OK...*, um die Installation abzuschließen.

Beim Novell iManager einloggen

Nach der Installation können Sie sich via Web-Browser mithilfe der folgenden URL am iManager einloggen:

https://<IP-Adresse des eDirectory-Servers>:8443/nps

Novell empfiehlt die Verwendung der Web-Browser Microsoft Internet Explorer oder Mozilla Firefox. In Mozilla Firefox werden möglicherweise nicht alle Popup-Fenster des Kontext-Menüs angezeigt.

ConsoleOne installieren und starten

Mit ConsoleOne steht Ihnen ein weiteres Administrationstool von Novell eDirectory zur Verfügung.

Zur Installation von ConsoleOne gehen Sie wie folgt vor:

- Melden Sie sich mit Root-Berechtigung (Super User) am eDirectory Server an.
- Wechseln Sie in das Verzeichnis */home/eDirectory*:

  ```
  cd /home/eDirectory
  ```

- Extrahieren Sie das ConsoleOne-Archiv *c1_136f-linux.tar.gz*:

  ```
  tar -xzvf c1_136f-linux.tar.gz
  ```

  Nach der Extraktion enthält */home/eDirectory* ein neues Verzeichnis *Linux*.

- Wechseln Sie in das Verzeichnis *Linux*:

  ```
  cd Linux
  ```

- Rufen Sie das Installationsskript *c1-install* auf:

  ```
  ./c1-install
  ```

- Wählen Sie die Sprache, in der die Installationsmeldungen ausgegeben werden sollen.
- Geben Sie „8“ für die Installation aller Snap-Ins ein.

ConsoleOne benötigt den Pfad zu einer installierten Java-Laufzeitumgebung. Den entsprechenden Pfadnamen können Sie in die Umgebungsvariable *C1_JRE_HOME* exportieren. Demgegenüber erfordert der systemweite Export des Pfadnamens Änderungen in der *bash*-Profile.

Da Root-Berechtigung für das Arbeiten mit ConsoleOne erforderlich ist, genügt es im Prinzip, den Pfadnamen nur für die Kennung *superuser Root* zu exportieren. Im Folgenden ist jedoch der systemweite Export des Pfadnamens dargestellt. Damit können auch normale Benutzer mit ConsoleOne arbeiten, sofern sie Root-Berechtigung besitzen.

Gehen Sie wie folgt vor:

- Öffnen Sie die Ihre Konfigurationsdatei zur Bearbeitung (im Beispiel: */etc/bash.bashrc*)
- Fügen Sie in der Konfigurationsdatei vor „# End of ...“ die folgende Zeile ein:

```
export C1_JRE_HOME=/opt/novell/j2sdk1.4.2_05/jre
```

Hier wird die zusammen mit eDirectory installierte Java-Laufzeitumgebung verwendet. Sie können aber auch den Pfadnamen einer beliebigen anderen auf dem eDirectory Server installierten Java-Laufzeitumgebung angeben.

ConsoleOne erhält die verfügbaren Baumstrukturen entweder über die lokale Konfigurationsdatei *hosts.nds* oder über den SLP-Service und Multicast.

Zum Einfügen Ihrer Baumstruktur in die Konfigurationsdatei gehen Sie verfahren Sie wie folgt:

- Wechseln Sie in Ihr Konfigurationsverzeichnis:

```
cd /etc
```

- Erzeugen Sie die Datei *hosts.nds*, falls Sie noch nicht existiert.
- Öffnen Sie die Datei *hosts.nds* und fügen Sie die folgenden Zeilen ein:

```
#Syntax: TREENAME.FQDN:PORT
MY_Tree.mycomputer.mydomain:81
```

ConsoleOne starten

ConsoleOne starten Sie in der System-Eingabeaufforderung mit folgendem Kommando:

```
/usr/ConsoleOne/bin/ConsoleOne
```

8.2.6.3 Novell eDirectory konfigurieren

Zur Konfiguration von Novell eDirectory führen Sie die folgenden Schritte durch:

1. NDS-Baum erzeugen.
2. eDirectory für LDAP konfigurieren.
3. Zugang zu eDirectory via LDAP-Browser testen.

NDS-Baum erzeugen

Einen NDS (**N**etwork **D**irectory **S**ervice)-Baum erzeugen Sie mit dem Utility ndsmanage. ndsmanage benötigt hierfür die folgenden Informationen:

TREE NAME
: Netzweit eindeutiger Name für den neuen NDS-Baum, z.B. *MY_TREE*.

Server Name
: Name einer Instanz der Klasse *server* in eDirectory. Für *Server Name* spezifizieren Sie den Namen des PRIMERGY Servers, auf dem der LDAP-Server läuft, z.B. *lin36-root-0*.

Server Context
: Fully Distinguished Name (vollständige Beschreibung von Objektpfad und der Attributen) des Containers, in dem das *Server* Objekt enthalten ist, z.B. *dc=organization.dc=mycompany*.

Admin User
: Fully Distinguished Name (vollständige Beschreibung von Objektpfad und der Attributen) des administrationsberechtigten Benutzers, z.B. *cn=admin.dc=organization.dc=mycompany*

NCP Port
: Spezifizieren Sie den Port 81.

Instance Location
: Spezifizieren Sie als Pfad: */home/root/instance0*

Configuration File
: Spezifizieren Sie folgende Datei: */home/root /instance0/ndsconf*

Password for admin user
: Geben Sie hier das Administratorpasswort an.

Zur Konfigurierung des NDS-Baums gehen Sie wie folgt vor:

- ► Öffnen Sie eine Command Box.
- ► Wechseln Sie in das Verzeichnis */home/eDirectory*.
- ► Starten Sie das Utility ndsmanage durch Eingabe des Kommandos *ndsmanage*:

  ```
  ndsmanage
  ```

- ► Geben Sie „c“ ein für die Erzeugung einer neuen Instanz der Klasse *server*.
- ► Geben Sie „y“ ein , um die Konfiguration fortzusetzen.
- ► Geben Sie „y“ ein, um einen neuen Baum zu erzeugen.

  Anschließend erfragt ndsmanage nacheinander die Werte für *TREE NAME*, *Server Name*, *Server Context* etc. (siehe Seite 271).

  Sobald die Eingabe abgeschlossen ist, konfiguriert ndsmanage den NDS-Baum.

- ► Führen Sie nach Abschluss der Konfiguration des NDS-Baums einen Neustart des PRIMERGY Servers durch, um die Konfiguration zu aktivieren, d.h. den NDS-Baum zu erzeugen.

eDirectory für LDAP konfigurieren

Die Konfiguration von eDirectory für LDAP umfasst die folgenden Schritte:

- – Role Based Services (RBS) installieren.
- – Plugin-Module installieren.
- – Role Based Services (RBS) konfigurieren.
- – eDirectory mit/ohne SSL/TLS-Unterstützung konfigurieren.

Im Einzelnen gehen Sie wie folgt vor:

- ► Loggen Sie sich beim iManager via Web-Browser unter der Administratorkennung (*Admin*) ein.

Role Based Services (RBS) installieren

RBS installieren Sie mithilfe des iManager Configuration Wizard.

Gehen Sie wie folgt vor:

- Wählen Sie im iManager die Registerkarte *Configure* (durch Klicken auf das Desk-Symbol).
- Wählen Sie in der Registerkarte *Configure*:
  Role Based Services - *RBS Configuration*
- Starten Sie den RBS Configuration Wizard.
- Weisen *RBS2* dem zu verwaltenden Container zu. (Im obigen Beispiel ist dies „mycompany“.)

Plugin-Module installieren

Gehen Sie wie folgt vor:

- Wählen Sie im iManager die Registerkarte *Configure* (durch Klicken auf das Desk-Symbol).
- Wählen Sie in der Registerkarte *Configure*:
  Plug-in installation - *Available Novell Plug-in Modules*
- Wählen Sie in der Seite *Available Novell Plug-in Modules* unter den aufgelisteten Modulen das eDirectory-spezifische Package *eDir_88_iMan26_Plugins.npm*.
- Klicken Sie auf *Install*.

Role Based Services (RBS) konfigurieren

- Wählen Sie in der Seite *Available Novell Plug-in Modules* alle für die LDAP-Integration benötigten Module. Falls Sie sich nicht sicher sind, wählen Sie alle Module.
- Klicken Sie auf *Install*.

eDirectory für SSL/TLS gesicherten Zugriff konfigurieren

Während der eDirectory-Installation wird ein temporäres Zertifikat erzeugt, sodass der Zugriff auf eDirectory standardmäßig durch SSL/TLS abgesichert ist. Da jedoch die Firmware des iRMC S4 für die Verwendung von RSA/MD5-Zertifikaten konfiguriert ist, benötigt die SSL/TLS gesicherte globale iRMC S4-Benutzerverwaltung via eDirectory ein RSA/MD5 Zertifikat der Länge 1024 byte.

Ein RSA/MD5-Zertifikat der Länge 1024 byte erstellen Sie wie folgt mithilfe von ConsoleOne:

- Loggen Sie sich am LDAP-Server unter Ihrer Administratorkennung (*Admin*) ein und starten Sie ConsoleOne.
- Navigieren Sie zum Root-Verzeichnis Ihrer Unternehmensstruktur (z.B. *baumname/mycompany/myorganisation*).
- Wählen Sie *New Object - NDSPKI key material - custom*, um ein neues Objekt der Klasse *NDSPKI:Key Material* zu erstellen.
- Spezifizieren Sie im nachfolgenden Dialog die folgenden Werte:

  1. 1024 bits
  2. SSL or TLS
  3. signature RSA/MD5

  Ein neues Zertifikat des gewünschten Typs wird erstellt.

Um das neu erstellte Zertifikat für die SSL-gesicherte LDAP-Verbindung zu aktivieren führen Sie im iManager die folgenden Schritte durch:

- Starten Sie den iManager via Web-Browser.
- Loggen Sie sich beim iManager mit gültigen Authentisierungsdaten ein.
- Wählen Sie *LDAP - LDAP Options - LDAP Server - Connection*.

  Die Registerkarte *Connection* enthält eine Drop down-Liste, die alle auf dem System installierten Zertifikate anzeigt.
- Selektieren Sie in der Drop down-Liste das gewünschte Zertifikat.

eDirectory für den nicht-SSL-gesicherten Zugriff konfigurieren

Anonymes Login sowie die Übertragung von Klartext-Passwörtern über ungesicherte Kanäle sind in eDirectory standardmäßig deaktiviert. Demzufolge ist das Einloggen via Web-Browser am eDirectory-Server nur über eine SSL-Verbindung möglich.

Für die Nutzung von LDAP ohne SSL müssen Sie die folgenden Schritte durchführen:

1. Nicht-SSL-gesicherte LDAP-Verbindung ermöglichen.
2. Bind-Restriktionen lockern.
3. LDAP-Konfiguration neu laden.

Gehen Sie wie folgt vor:

1. Nicht-SSL-gesicherte LDAP-Verbindung ermöglichen.
   - ► Starten Sie den iManager via Web-Browser.
   - ► Loggen Sie sich beim iManager mit gültigen Authentisierungsdaten ein.
   - ► Wählen Sie den *Roles and Tasks*-View.
   - ► Wählen Sie *LDAP - LDAP Options - LDAP Server - Connection*.
   - ► Deaktivieren in der Registerkarte *Connection* die Option *Require TLS for all Operations.*
   - ► Wählen Sie *LDAP - LDAP Options - LDAP Group - General*.
   - ► Deaktivieren die in der Registerkarte *General* die Option *Require TLS for Simple Binds with password.*
2. Bind-Restriktionen lockern.
   - ► Loggen Sie sich beim iManager mit gültigen Authentisierungsdaten ein.
   - ► Navigieren Sie im Objekt-Baum zum *LDAP Server*-Objekt.
   - ► Markieren Sie das *LDAP Server*-Objekt per Maus-Klick und wählen Sie *Modify Object* im zughörigen Kontext-Menü.
   - ► Öffnen Sie im rechten Content-Frame das *Other*-Sheet.
   - ► Wählen Sie unter *Valued Attributes*: *ldapBindRestrictions*
   - ► Klicken Sie auf die Schaltfläche *Edit*.
   - ► Setzen Sie den Wertauf „0“.
   - ► Klicken Sie auf die Schaltfläche *OK*.
   - ► Klicken Sie im *Other*-Sheet auf die Schaltfläche *Apply*.
3. LDAP-Konfiguration neu laden.
   - ► Starten Sie ConsoleOne und loggen Sie sich in eDirectory ein.
   - ► Klicken Sie auf der links im Fenster auf das *Base DN*-Objekt (z.B. *Mycompany*). Auf der rechten Fensterseite wird daraufhin das *LDAP Server*-Objekt angezeigt.
   - ► Markieren Sie das *LDAP Server*-Objekt per Klick mit der rechten Maustaste und selektieren Sie *Properties...* im zughörigen Kontext-Menü.
   - ► Klicken Sie in der Registerkarte *General* auf *Refresh NLDAP Server Now*.

Zugriff auf eDirectory via LDAP Browser testen

Nach erfolgreicher Durchführung der oben beschriebenen Schritte 1 - 3 sollten Sie via LDAP Browser-Utility eine Verbindung zu eDirectory herstellen können. Mit dem LDAP-Browser von Jarek Gavor (siehe Seite 293) können Sie dies wie folgt testen:

- Versuchen Sie, sich unter der Administratorkennung (im Beispiel: *admin*) über eine SSL-Verbindung in eDirectory einzuloggen.

Falls der Versuch fehlschlägt, verfahren Sie wie folgt:

- Prüfen Sie, ob SSL aktiviert ist (vergleiche Seite 274).

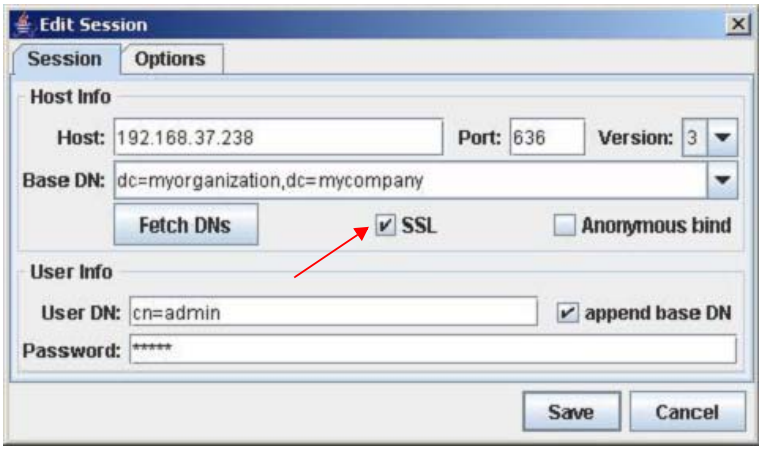


Bild 74: LDAP-Zugriff auf eDirectory testen: SSL aktiviert

- Versuchen Sie, sich unter der Administratorkennung (im Beispiel: *admin*) über eine nicht SSL-gesicherte Verbindung in eDirectory einzuloggen.

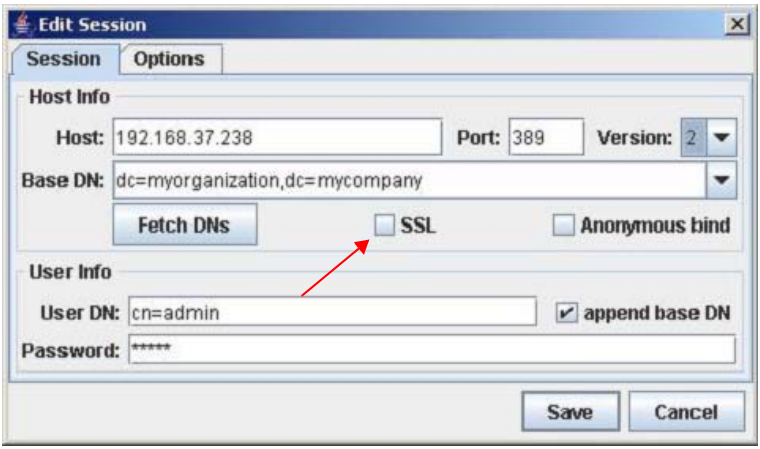


Bild 75: LDAP-Zugriff auf eDirectory testen: SSL nicht aktiviert

- Falls die Anmeldung erneut fehlschlägt:
  Lockern Sie die Bind-Restriktionen (siehe Seite 274).

8.2.6.4 iRMC S4-Benutzerverwaltung in Novell eDirectory integrieren

Voraussetzung:

Eine LDAP v1 und/oder eine LDAP v2-Struktur ist im eDirectory-Verzeichnisdienst generiert (siehe Abschnitt "SVS_LdapDeployer - Struktur „SVS“ generieren, pflegen und löschen" auf Seite 242).

Für die Integration der iRMC S4-Benutzerverwaltung in Novell eDirectory sind die folgenden Schritte erforderlich:

– Principal iRMC User erzeugen.

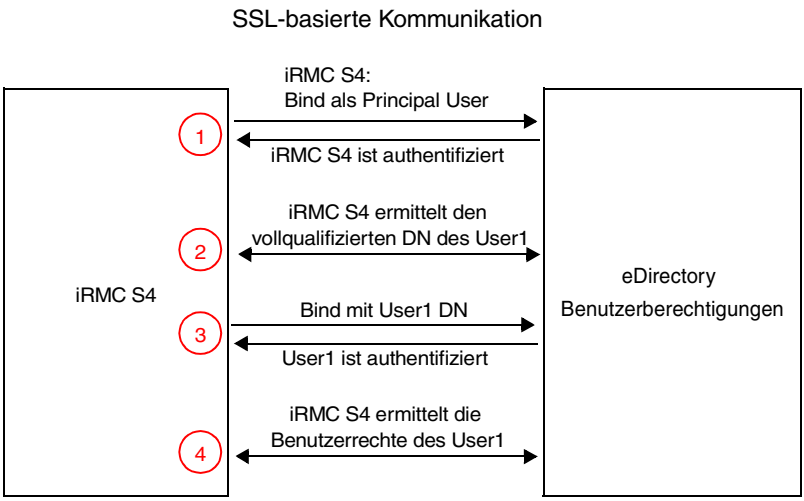
– iRMC-Gruppen und Benutzerrechte in eDirectory vereinbaren.

– Benutzer den Berechtigungsgruppen zuordnen.

LDAP-Authentifizierungsprozess für iRMC S4-Benutzer in eDirectory

Die Authentifizierung eines globalen iRMC S4-Benutzers beim Login am iRMC S4 erfolgt nach einem fest vorgegebenen Schema (siehe Seite 230). Bild 76 auf Seite 278 veranschaulicht diesen Prozess für die globale iRMC S4-Benutzerverwaltung mithilfe von Novell eDirectory.

Das Herstellen einer Verbindung und die Anmeldung mit entsprechenden Anmeldeinformationen wird als BIND-Operation bezeichnet.



1) Der iRMC S4 loggt sich am eDirectory-Server mit vordefinierten, bekannten Berechtigungsdaten (iRMC-Einstellung) als „Principal User“ ein und wartet auf den erfolgreichen Bind.

2) Der iRMC S4 erfragt vom eDirectory-Server den voll-qualifizierten Distinguished Name (DN) des Benutzers mit „cn=User1“. eDirectory ermittelt den DN aus dem vorkonfigurierten Teilbaum (iRMC-Einstellung).

3) Der iRMC S4 loggt sich am eDirectory-Server mit dem vollqualifizierten DN des Benutzers User1 ein und wartet auf den erfolgreichen Bind.

4) Der iRMC S4 erfragt vom eDirectory-Server die Benutzerberechtigungen des Benutzers User1.

Bild 76: Authentifizierungsschema für globale iRMC S4-Benutzerberechtigungen

Die Berechtigungsdaten des „Principal User“ sowie den Teilbaum, der die DNs enthält, konfigurieren Sie in der Seite *Directory Service Configuration* der iRMC S4-Web-Oberfläche (siehe Handbuch "iRMC S4 - integrated Remote Management Controller").

Der CN eines Benutzers muss innerhalb des durchsuchten Teilbaums eindeutig sein.

Principal User (Principal Benutzer) für den iRMC S4 erzeugen

Um einen Principal User für den iRMC S4 zu erzeugen, gehen Sie wie folgt vor:

- Loggen Sie sich mit gültigen Authentisierungsdaten beim iManager ein.
- Wählen Sie *Roles and Tasks*.
- Wählen Sie *Users - Create User*.
- Tragen Sie die erforderlichen Angaben in das angezeigte Template ein.

  Distinguished Name (DN) und Passwort des Principal Users müssen mit entsprechenden Angaben für die Konfiguration des iRMC S4 übereinstimmen (siehe Handbuch "iRMC S4 - integrated Remote Management Controller").

  Der *Context:* des Benutzers kann sich an beliebiger Stelle im Baum befinden.

- Erteilen Sie dem Principal User Suchberechtigung für die folgenden Teilbäume:
  - Teilbaum (OU) *SVS*
  - Teilbaum (OU), der die Benutzer enthält (z.B. *people*).

Den iRMC-Gruppen und -Benutzern Benutzerrechte erteilen

Standardmäßig verfügt ein Objekt in eDirectory nur über sehr eingeschränkte Abfrage- und Suchberechtigungen in einem LDAP-Baum. Damit ein Objekt alle Attribute in einem oder mehreren Teilbäumen abfragen kann, müsse Sie diesem Objekt die entsprechenden Rechte zuweisen.

Berechtigungen erteilen Sie wahlweise einem einzelnen Objekt (d.h. einem speziellen Benutzer) oder einer Gruppe von Objekten, die in einer Organizational Unit (OU) wie z.B. *SVS* oder *people* zusammengefasst sind. Dabei gehen Berechtigungen, die einer OU erteilt und als „inherited“ gekennzeichnet sind, automatisch auf die Objekte dieser Gruppe über.

Für die Integration der iRMC S4-Benutzerverwaltung in Novell eDirectory ist es erforderlich, folgenden Objekten (Trustees) Suchberechtigung zu erteilen:

- *Principal User*
- Teilbaum, der die iRMC S4-Benutzer enthält

Wie Sie dabei im Einzelnen vorgehen ist nachfolgend beschrieben.

Um einem Objekt die Suchberechtigung für alle Attribute zu erteilen, verfahren Sie wie folgt:

- Starten Sie den iManager via Web-Browser.
- Loggen Sie sich beim iManager mit gültigen Authentisierungsdaten ein.
- Klicken Sie im iManager auf die Schaltfläche *Roles and Tasks*.
- Wählen Sie im Menübaum *Rights - Rights to Other Objects*.

  Die Seite *Rights to Other Objects* wird angezeigt.
- Spezifizieren Sie unter *Trustee Name* den Namen des Objekts (in Bild 77 auf Seite 281 *SVS.sbdr4*), dem die Berechtigung erteilt werden soll.
- Spezifizieren Sie unter *Context to Search From* den eDirectory-Teilbaum (*SVS*), den der iManager nach allen Objekten durchsuchen soll, für die der Trustee *Users* zurzeit leseberechtigt ist.
- Klicken Sie auf die Schaltfläche *OK*.

  Eine Fortschrittanzeige informiert über den Stand der Suche. Nach Abschluss des Suchvorgangs wird die Seite *Rights to Other Objects* angezeigt, die jetzt das Suchergebnis enthält (siehe Bild 77 auf Seite 281).

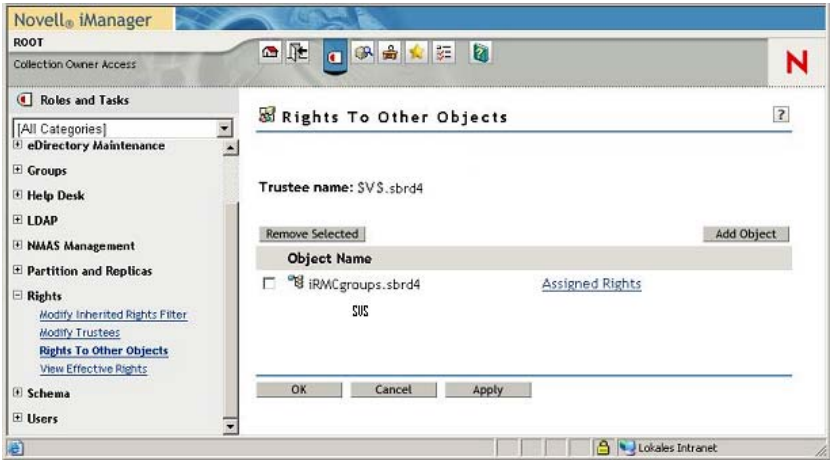


Bild 77: iManager - Roles and Tasks - Rights To Other Objects

Falls unter *Object Name* kein Objekt angezeigt wird, hat der Trustee zurzeit keine Berechtigung innerhalb des angegebenen Kontexts.

► Erteilen Sie dem Trustee gegebenenfalls zusätzliche Berechtigung(en):

► Klicken Sie auf *Add Object*.

► Selektieren Sie via Objektselektor-Schaltfläche das Objekt, für das Sie dem Trustee eine Berechtigung erteilen wollen.

► Klicken Sie auf *Assigned Rights*.

Falls die Property *[All Attributes Rights]* nicht angezeigt wird:

► Klicken Sie auf *Add Property*.

Das *Add Property*-Fenster wird angezeigt (siehe Bild 78 auf Seite 282).

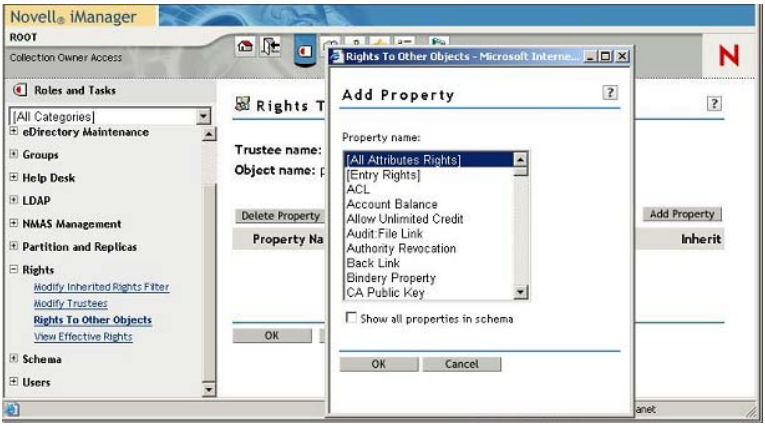


Bild 78: iManager - Roles and Tasks - Rights To Other Objects - Add Property

► Markieren Sie die Property *[All Attributes Rights]* und fügen Sie durch Klicken auf *OK* hinzu.

► Aktivieren Sie für die Property *[All Attributes Rights]* die Optionen *Compare*, *Read* und *Inherit* und bestätigen Sie mit *OK*.

Damit sind Benutzer/Benutzergruppe zur Abfrage aller Attribute im Teilbaum des ausgewählten Objekts autorisiert.

► Klicken Sie auf *Apply*, um Ihre Einstellungen zu aktivieren.

8.2.6.5 iRMC S4-Benutzer der Berechtigungsgruppe zuordnen

Die Zuordnung von iRMC S4-Benutzern (z.B. der OU *people*) zu iRMC S4-Berechtigungsgruppen können Sie wahlweise vornehmen

– ausgehend vom Benutzereintrag (günstig bei wenigen Benutzereinträgen) oder
– ausgehend vom Rolleneintrag / Gruppeneintrag (günstig bei vielen Benutzereinträgen).

Nachfolgend ist exemplarisch die Zuordnung von iRMC S4-Benutzern einer OU *people* zu einer Berechtigungsgruppe dargestellt. Erläutert wird dabei die vom Gruppeneintrag / Rolleneintrag ausgehende Zuordnung.

Die Zuordnung ausgehend vom Benutzereintrag verläuft weitgehend analog.

In eDirectory müssen die Benutzer „von Hand“ in die Gruppen eingetragen werden.

Gehen Sie wie folgt vor:

► Starten Sie den iManager via Web-Browser.

► Loggen Sie sich beim iManager mit gültigen Authentisierungsdaten ein.

► Wählen Sie *Roles and Tasks*.

► Wählen Sie *Groups - Modify Group*.

Die Seite *Modify Group* wird angezeigt.

► Führen Sie die folgenden Schritte für alle Berechtigungsgruppen durch, denen Sie iRMC S4-Benutzer zuordnen wollen:

► Selektieren Sie via Objektselektor-Schaltfläche die Berechtigungsgruppe, der Sie iRMC S4-Benutzer hinzufügen wollen (siehe Bild 79 auf Seite 284):
Administrator.AuthorizationRoles.DeptX.Departments.SVS.sbrd4

► Wählen Sie die Registerkarte *Members*.

Die Registerkarte *Members* der Seite *Modify Group* wird angezeigt:

Bild 79: iManager - Roles and Tasks - Modify Group - Registerkarte „Members“ (LDAP v2)

► Führen Sie den folgenden Schritt für alle Benutzer der OU *people* durch, die Sie der ausgewählten iRMC-Gruppe zuordnen wollen:

► Klicken Sie auf die Objektselektor-Schaltfläche .

Das *Object Selector (Browser)*-Fenster wird geöffnet (siehe Bild 80 auf Seite 285).

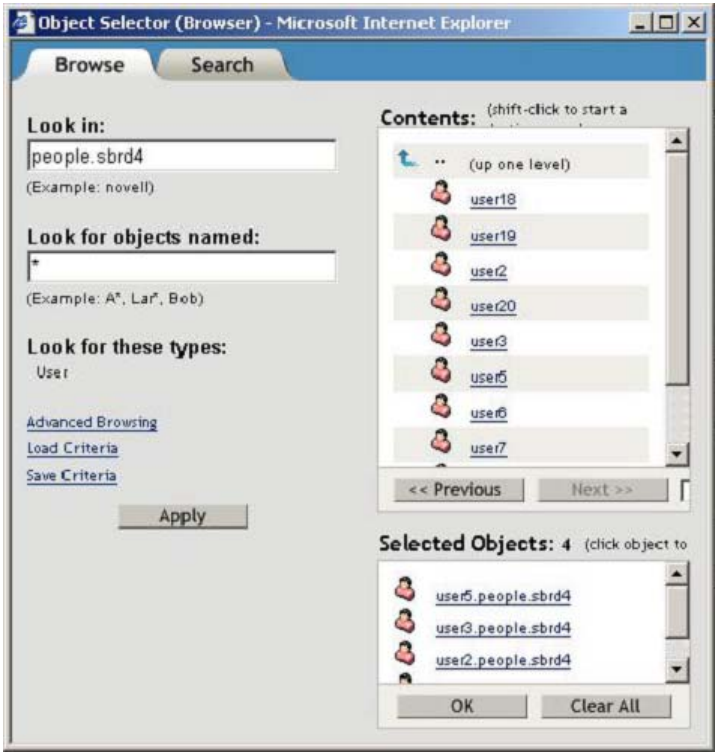


Bild 80: Benutzer der iRMC-Gruppe zuordnen - Benutzer auswählen

► Selektieren Sie im *Object Selector (Browser)*-Fenster den/die gewünschten Benutzer der OU *people* und bestätigen Sie Ihre Auswahl mit *OK*.

Im Anzeigebereich der Registerkarte *Members* der Seite *Modify Group* werden die ausgewählten Benutzer angezeigt (siehe 81 auf Seite 286).

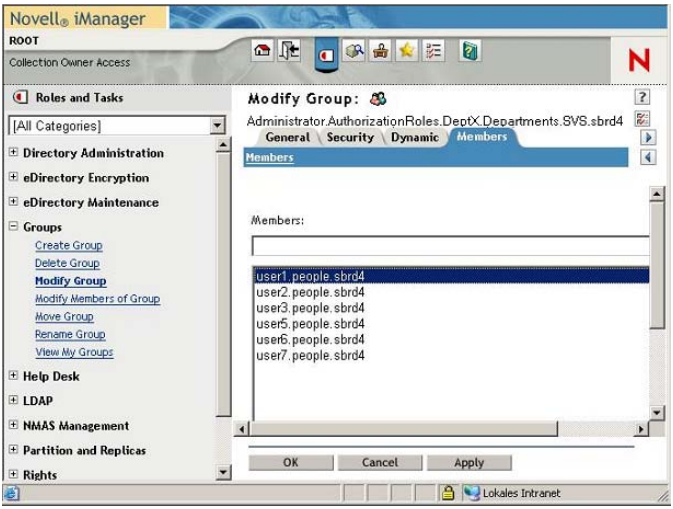


Bild 81: Anzeige der ausgewählten iRMC S4-Benutzer in der Registerkarte „Members (LDAP v2)

► Bestätigen Sie mit *Apply* oder *OK*, um die ausgewählten Benutzer zur iRMC-Gruppe (hier: ... .*SVS.sbdr4*) hinzuzufügen.

8.2.6.6 Tipps zur Administration von Novell eDirectory

NDS-Dämon neu starten

Für einen Neustart des NDS-Dämons gehen Sie wie folgt vor:

- ► Öffnen Sie die Command Box.
- ► Melden Sie sich mit Root-Berechtigung an.
- ► Führen Sie das folgende Kommando aus:

```
rcndsd restart
```

Falls sich der nldap-Dämon ohne ersichtlichen Grund nicht starten lässt:

- ► Starten Sie den *lndap*-Dämon „von Hand“:

```
/etc/init.d/nldap restart
```

Falls der iManager nicht reagiert:

- ► Starten Sie den iManager neu:

```
/etc/init.d/novell-tomcat4 restart
```

Konfiguration des NLDAP-Servers neu laden

Gehen Sie wie folgt vor:

- ► Starten Sie ConsoleOne und loggen Sie sich in eDirectory ein.

  Wenn Sie ConsoleOne zum ersten Mal starten, ist noch kein Baum konfiguriert.

  Zur Konfiguration eines Baums gehen Sie wie folgt vor:

  - ► Wählen Sie unter *My World* den Knoten *NDS*.
  - ► Wählen Sie in der Menü-Leiste: *File - Authenticate*
  - ► Geben Sie für das Login die folgenden Authentisierungsdaten ein:
    1. Login-Name: root
    2. Passwort: <passwort>
    3. Tree: MY_TREE
    4. Context: mycompany

- ► Klicken Sie links im Fenster auf das *Base DN*-Objekt (*Mycompany*).

  Auf der rechten Fensterseite wird dann das *LDAP Server*-Objekt angezeigt.

- ► Klicken Sie mit der rechten Maustaste auf das *LDAP Server*-Objekt und wählen Sie *Properties...* im Kontext-Menü.

- ► Klicken Sie in der Registerkarte *General* auf die Schaltfläche *Refresh NLDAP Server Now*.

NDS Meldungs-Trace konfigurieren

Der *nds*-Dämon erzeugt Debug-und Log-Meldungen, die Sie mit dem Tool *ndstrace* verfolgen können. Zweck der im Folgenden beschriebenen Konfiguration ist es, den Terminal-Output von *ndstrace* in eine Datei umzuleiten und sich den Inhalt dieser Datei an einem anderen Terminal anzeigen zu lassen. Für Letzteres verwenden Sie das Tool *screen*.

Es empfiehlt sich folgende Vorgehensweise:

- ► Öffnen Sie die Command Box (z.B. *bash*).

ndstrace konfigurieren

- ► Wechseln Sie in das eDirectory-Verzeichnis */home/eDirectory*:

  ```
  cd /home/eDirectory
  ```

- ► Starten Sie *screen* mit dem Kommando `screen`.

- ► Starten Sie *ndstrace* mit dem Kommando `ndstrace`.

- ► Selektieren Sie die Module, die Sie aktivieren wollen.

  Wollen Sie sich z.B. die Zeitpunkte anzeigen lassen wollen, an denen Ereignisse eingetreten sind, dann geben Sie `dstrace TIME` ein.

  Es wird dringend empfohlen, die Module *LDAP* und *TIME* durch zu folgende Eingabe zu aktivieren:

  ```
  dstrace LDAP TIME
  ```

- ► Beenden *ndstrace* durch Eingabe von *quit*.

  Damit ist die Konfiguration von *ndstrace* abgeschlossen.

Meldungsausgabe auf zweites Terminal umleiten

- Starten Sie *ndstrace* und leiten Sie die Meldungsausgebe um:

  ```
  ndstrace -l >ndstrace.log
  ```

- Öffnen Sie ein zweites Terminal mithilfe der folgenden Tastenkombination: Ctrl + a, Crtl + c
- Schalten Sie den Mitschnitt der Protokollierung ein:

  ```
  tail -f ./ndstrace.log
  ```

- Um zwischen den virtuellen Terminals hin- und herzuschalten, verwenden Sie die Tastenkombination Ctrl + a, Crtl + 0.
  (Die Terminals sind von 0 bis 9 durchnummeriert.)

8.2.7 iRMC S4-Benutzerverwaltung via OpenLDAP

Dieser Abschnitt informiert über die folgenden Themen:

– OpenLDAP installieren (Linux).

– SSL-Zertifikat erzeugen.

– OpenLDAP konfigurieren.

– iRMC S4-Benutzerverwaltung in OpenLDAP integrieren.

– Tipps zur Administration von OpenLDAP

8.2.7.1 OpenLDAP installieren

Vor der Installation von OpenLDAP müssen Sie die Firewall für Verbindungen zu den Ports 389 und 636 konfigurieren.

Bei OpenSuSE verfahren Sie hierfür wie folgt:

► Ergänzen Sie in der Datei */etc/sysconfig/SuSEfirewall2* die Option *FW_SERVICES_EXT_TCP* wie folgt:

```
FW_SERVICES_EXT_TCP="389 636"
```

Zur Installation der Packages *OpenSSL* und *OpenLDAP2* vom Distributionsmedium verwenden Sie das Setup-Tool YaST.

8.2.7.2 SSL-Zertifikate erzeugen

Es soll ein Zertifikat mit folgenden Eigenschaften erzeugt werden:

– Schlüssellänge: 1024 bit
– md5RSAEnc

Schlüsselpaare und signierte Zertifikate (selbstsigniert oder von einer externen CA signiert) erzeugen Sie mithilfe von OpenSSL. Nähere Informationen hierzu finden Sie auf der OpenSSL-Homepage unter *http://www.openssl.org*.

Unter den folgenden Links finden Sie Anleitungen zur Einrichtung einer CA und zum Erstellen von Test-Zertifikaten:

– *http://www.akadia.com/services/ssh_test_certificate.html*
– *http://www.freebsdmadeeasy.com/tutorials/web-server/apache-ssl-certs.php*
– *http://www.flatmtn.com/computer/Linux-SSLCertificates.html*
– *http://www.tc.umn.edu/~brams006/selfsign.html*

Als Ergebnis der Zertifikatserstellung müssen die folgenden drei PEM-Dateien vorliegen:

– Root-Zertifikat: *root.cer.pem*

– Server-Zertifikat: *server.cer.pem*

– Private Key: *server.key.pem*

Der Private Key **darf nicht** mit einer Passphrase verschlüsselt sein, da Sie **nur dem LDAP-Dämon** (*ldap*) Leseberechtigung für die Datei *server.key.pem* erteilen sollten.

Die Passphrase entfernen Sie mit folgendem Kommando:

```
openssl rsa –in server.enc.key.pem –out server.key.pem
```

8.2.7.3 OpenLDAP konfigurieren

Zur Konfiguration von OpenLDAP gehen Sie wie folgt vor:

- Starten Sie das Setup-Tool Yast und wählen Sie *LDAP-Server-Configuration*.
- Aktivieren Sie unter *Global Settings/Allow Settings* die Einstellung *LDAPv2-Bind*.
- Wählen Sie *Global Settings/TLS Settings*:
  - Aktivieren Sie die Einstellung *TLS*.
  - Geben Sie die Pfade der bei der Installation erstellten Dateien bekannt (siehe Abschnitt "OpenLDAP installieren" auf Seite 290).
  - Stellen Sie sicher, dass Zertifikate und Privater Schlüssel im Dateisystem vom LDAP-Service gelesen werden können.

    Da *openldap* unter der *uid/guid=ldap* ausgeführt wird, können Sie dies z.B. erreichen, indem Sie

    – den Eigentümer der Dateien mit Zertifikaten und privaten Schlüsseln auf „ldap“ setzen oder

    – dem LDAP-Dämon *ldap* die Leseberechtigung auf die Dateien mit Zertifikaten und privaten Schlüsseln erteilen.
- Wählen Sie *Databases*, um eine neue Datenbank zu erzeugen.

Falls die von YaST erstellte Konfiguration generell nicht funktioniert, prüfen Sie die Konfigurationsdatei */etc/openldap/slapd.conf* auf folgende zwingend erforderlichen Einträge:

```
allow bind_v2

TLSCACertificateFile /path/to/ca-certificate.pem

TLSCertificateFile /path/to/certificate.pem

TLSCertificateKeyFile /path/to/privat.key.pem
```

Falls die von YaST erstellte Konfiguration für SSL nicht funktioniert, prüfen Sie die Konfigurationsdatei */etc/sysconfig/openldap* auf folgenden Eintrag:

```
OPENLDAP_START_LDAPS=“yes“
```

8.2.7.4 iRMC S4-Benutzerverwaltung in OpenLDAP integrieren

Voraussetzung:

Eine LDAP v1 und/oder eine LDAP v2-Struktur ist im OpenLDAP-Verzeichnisdienst generiert (siehe Abschnitt "SVS_LdapDeployer - Struktur „SVS“ generieren, pflegen und löschen" auf Seite 242).

Die Integration der iRMC S4-Benutzerverwaltung in OpenLDAP umfasst die folgenden Schritte:

– Principal iRMC User erzeugen.

– Neuen iRMC S4-Benutzer erzeugen und der Berechtigungsgruppe zuordnen.

Verwenden Sie zur Erzeugung des Principal User (ObjectClass: *Person*) einen LDAP-Browser, z.B. den LDAP Browser\Editor von Jarek Gawor (siehe Seite 293).

LDAP Browser\Editor von Jarek Gawor

Den LDAP Browser\Editor von Jarek Gawor können Sie über eine grafische Oberfläche einfach bedienen. Das Tool steht im Internet zum Download zur Verfügung.

Zur **Installation des LDAP Browser\Editor** verfahren Sie wie folgt:

- Entpacken Sie das Zip-Archiv *Browser281.zip* in ein Installationsverzeichnis Ihrer Wahl.
- Setzen Sie die Umgebungsvariable *JAVA_HOME* auf das Installationsverzeichnis der JAVA-Laufzeitumgebung, z.B.:

  ```
  JAVA_HOME=C:\Programme\Java\jre7
  ```

Principal User (Principal Benutzer) erzeugen

Verwenden Sie zur Erzeugung des Principal User (ObjectClass: *Person*) einen LDAP-Browser, z.B. den LDAP Browser\Editor von Jarek Gawor (siehe Seite 293).

Im Folgenden ist beschrieben, wie Sie den Principal User mithilfe des LDAP Browser\Editor von Jarek Gawor erzeugen.

Gehen Sie wie folgt vor:

- Starten Sie den LDAP Browser.
- Loggen Sie sich beim OpenLDAP-Verzeichnisdienst mit gültigen Authentisierungsdaten ein.
- Wählen Sie den Teilbaum (Untergruppe), in dem der Principal User angelegt werden soll. Der Principal User kann an beliebiger Stelle dieses Baums angelegt werden.
- Öffnen Sie das Menü *Edit*.
- Wählen Sie *Add Entry*.
- Wählen Sie *Person*.
- Ändern Sie den Distinguished Name *DN*.

  Distinguished Name (DN) und Passwort des Principal User müssen mit entsprechenden Angaben für die Konfiguration des iRMC S4 übereinstimmen (siehe Handbuch "iRMC S4 - integrated Remote Management Controller").
- Klicken Sie auf *Set* und geben Sie ein Passwort ein.
- Geben Sie einen Sur Name *SN* ein.
- Klicken Sie auf *Apply*.

Neuen iRMC S4-Benutzer erzeugen und den Berechtigungsgruppen zuordnen

Verwenden Sie für Erzeugung eines neuen Benutzers (ObjectClass *Person*) sowie zur Zuordnung eines Benutzers zur Berechtigungsgruppe einen LDAP-Browser, z.B. den LDAP Browser\Editor von Jarek Gawor (siehe Seite 293).

Im Folgenden ist beschrieben, wie Sie mithilfe des LDAP Browser\Editor von Jarek Gawor einen neuen iRMC S4-Benutzer erzeugen und ihn zur Berechtigungsgruppe hinzufügen.

Gehen Sie wie folgt vor:

- Starten Sie den LDAP Browser.
- Loggen Sie sich beim OpenLDAP-Verzeichnisdienst mit gültigen Authentisierungsdaten ein.
- Erzeugen Sie einen neuen Benutzer:

  Gehen Sie hierbei wie folgt vor:

  - Wählen Sie den Teilbaum (Untergruppe), in dem der neue Benutzer angelegt werden soll. Der neue Benutzer kann an beliebiger Stelle des Baums angelegt werden.
  - Öffnen Sie das Menü *Edit*.
  - Wählen Sie *Add Entry*.
  - Wählen Sie *Person*.
  - Ändern Sie den Distinguished Name *DN*.
  - Klicken Sie auf *Set* und geben Sie das Passwort ein.
  - Geben Sie einen Sur Name *SN* ein.
  - Klicken Sie auf *Apply*.

► Ordnen Sie den soeben erzeugten Benutzer der Berechtigungsgruppe zu.

Gehen Sie hierbei wie folgt vor:

► Wählen Sie den Teilbaum (Untergruppe) von *SVS*, dem der Benutzer angehören soll, d.h.

cn=UserKVM,ou=YourDepartment,ou=Departments,ou=SVS, dc=myorganisation,dc=mycompany

► Öffnen Sie das Menü *Edit*.

► Wählen Sie *Add Attribute*.

► Geben Sie als Attributnamen „Member“ ein. Als Wert geben Sie den vollqualifizierten DN zuvor erzeugten Benutzers an, also

cn=UserKVM,ou=YourDepartment,ou=Departments,ou=SVS, dc=myorganisation,dc=mycompany

8.2.7.5 Tipps zur Administration von OpenLDAP

LDAP-Service neu starten

Um den LDAP-Service neu zu starten, verfahren Sie wie folgt:

- Öffnen Sie die Command Box.
- Melden Sie sich mit Root-Berechtigung an.
- Geben Sie das folgende Kommando ein:

```
rcldap restart
```

Meldungsprotokollierung

Für das Meldungslogging nutzt der LDAP-Dämon das Syslog-Protokoll.

Die protokollierten Meldungen werden nur angezeigt, wenn in der Datei */etc/openldap/slapd.conf* ein Log-Level ungleich 0 eingestellt ist.

Erläuterungen zu den verschiedenen Leveln finden Sie unter:

http://www.zytrax.com/books/ldap/ch6/#loglevel

Tabelle 37 auf Seite 298 gibt einen Überblick über die Log-Level und ihre Bedeutung.

Log-Level	Bedeutung
-1	umfassendes Debugging
0	kein Debugging
1	Funktionsaufrufe protokollieren
2	Paketverarbeitung testen
4	Heavy Trace Debugging
8	Verbindungsmanagement
16	Gesendete und empfangene Pakete anzeigen
32	Suchfilterverarbeitung
64	Konfigurationsdateiverarbeitung
128	Verarbeitung der Zugangskontrolllisten
256	Status-Logging für Verbindungen / Operationen /Ergebnisse
512	Status-Logging für gesendete Einträge
1024	Kommunikation mit den Shell Backends ausgeben.
2048	Ergebnisse des Entry Parsings ausgeben.

Tabelle 37: OpenLDAP - Log-Level

8.2.8 E-Mail-Benachrichtigung an globale iRMC S4-Benutzer konfigurieren

Die E-Mail-Benachrichtigung an globale iRMC S4-Benutzer ist in die globale iRMC S4-Benutzerverwaltung integriert und kann somit zentral und Plattform-übergreifend über einen Verzeichnisserver konfiguriert und abgewickelt werden. Entsprechend konfigurierte globale Benutzerkennungen können E-Mail-Benachrichtigungen von allen iRMC S4 erhalten, die mit dem Verzeichnisserver im Netz verbunden sind.

Voraussetzungen

Für die E-Mail-Benachrichtigung müssen folgende Voraussetzungen erfüllt sein:

- Globale E-Mail-Benachrichtigung setzt eine iRMC S4-Firmware der Version 3.77A oder höher voraus, da eine LDAP v2-Struktur benötigt wird.
- In der iRMC S4-Web-Oberfläche muss ein Principal Benutzer konfiguriert sein, der berechtigt ist, im LDAP-Verzeichnisbaum (LDAP Tree) zu suchen (siehe Handbuch "iRMC S4 - integrated Remote Management Controller").
- Bei der Konfiguration der LDAP-Einstellungen auf der Seite *Verzeichnisdienst Konfiguration* muss unter *Verzeichnisdienst E-Mail Benachrichtigung* die E-Mail-Benachrichtigung konfiguriert sein (siehe Handbuch "iRMC S4 - integrated Remote Management Controller").

8.2.8.1 Globale E-Mail-Benachrichtigung

Die globale E-Mail-Benachrichtigung via Verzeichnisserver erfordert Benachrichtigungsgruppen (Alert Roles), die Sie zusätzlich zu den Authorization Roles in der Konfigurationsdatei des *SVS_LdapDeployer* (siehe Seite 242) definieren.

Benachrichtigungsgruppen (Alert Roles)

Eine Benachrichtigungsgruppe umfasst eine Auswahl definierter Benachrichtigungstypen (Alert Types, z.B. Temperaturüberschreitung) mit jeweils zugeordnetem Fehlergewicht (Severity, z.B. „kritisch“). Für Benutzer, die einer bestimmten Benachrichtigungsgruppe zugeordnet sind, legt die Benachrichtigungsgruppe fest, bei welchen Benachrichtigungstypen und Fehlergewichten die Benutzer per E-Mail benachrichtigt werden.

Die Syntax der Alert Roles ersehen Sie aus den Beispiel-Konfigurationsdateien *Generic_Settings.xml* und *Generic_InitialDeploy.xml*, die zusammen mit dem *jar*-Archiv *SVS_LdapDeployer.jar* auf der ServerView Suite DVD ausgeliefert werden.

Benachrichtigungstypen (Alert Types)

Folgende Benachrichtigungstypen werden unterstützt:

Benachrichtigungstyp	Ursache
FanSens	Lüfter-Sensoren
Temperat	Temperatur-Sensoren
HWError	Kritische Hardware-Fehler
Security	Sicherheit
SysHang	System-Hang
POSTErr	Systemstart-Fehler
SysStat	Systemstatus
DDCtrl	Festplatten und Controller
NetInterf	Netzwerk-Schnittstelle
RemMgmt	Remote Management
SysPwr	Energieverwaltung
Memory	Speicher
Others	Andere

Tabelle 38: Benachrichtigungstypen (Alert-Types)

Jedem Benachrichtigungstyp kann eines der folgenden Fehlergewichte (Severity Level) zugeordnet werden: *Warning*, *Critical*, *All*, (*none*).

Bevorzugter Mail Server

Bei globaler E-Mail-Benachrichtigung gilt für den bevorzugten Mail-Server die Einstellung *Automatic*: Falls die E-Mail nicht sofort erfolgreich versendet werden kann, weil z. B. der erste Mail-Server nicht verfügbar ist, wird E-Mail an den zweiten Mail-Server gesendet.

Unterstützte Mail-Formate

Es werden die folgenden Mail-Formate unterstützt:

- Standard
- Fixed Subject
- ITS-Format
- Fujitsu REMCS Format

Bei einem Mail-Format ungleich *Standard* müssen Sie die Benutzer der entsprechenden Mail-Format-Gruppe hinzufügen.

LDAP E-Mail-Tabelle

Wenn die E-Mail-Benachrichtigung konfiguriert ist (siehe Seite 303) und die Option *LDAP E-Mail aktiviert* gesetzt ist, sendet der iRMC S4 im Fall einer Alarmbenachrichtigung E-Mails an (siehe auch Handbuch "iRMC S4 - integrated Remote Management Controller").

- alle entsprechend konfigurierten lokalen iRMC S4-Benutzer,
- alle globalen iRMC S4-Benutzer, die in der LDAP E-Mail-Tabelle für diese Alarmbenachrichtigung registriert sind.

Die LDAP E-Mail-Tabelle wird in der iRMC S4-Firmware erstmalig beim Erst-Start des iRMC S4 angelegt und danach in regelmäßigen Abständen aktualisiert. Der Umfang der LDAP E-Mail-Tabelle ist begrenzt auf maximal 64 LDAP-Benachrichtigungsgruppen sowie auf maximal 64 globale iRMC S4-Benutzer, für die E-Mail-Benachrichtigung konfiguriert ist.

Es wird empfohlen, für die globale E-Mail-Benachrichtigung Email-Verteiler zu verwenden.

Für die E-Mail-Benachrichtigung ermittelt der LDAP-Verzeichnisserver aus der E-Mail-Tabelle folgende Informationen:

- Liste der globalen iRMC S4-Benutzer, für die E-Mail-Benachrichtigung konfiguriert ist.
- Für jeden globalen iRMC S4-Benutzer:
  - Liste der konfigurierten Alarmbenachrichtigungen des jeweiligen Alerts (Art und Fehlergewicht)
  - Gewünschtes Mail-Format

Die LDAP E-Mail-Tabelle wird bei folgenden Anlässen aktualisiert:

- Erst-/Neustart des iRMC S4
- Änderung der LDAP-Konfiguration
- In regelmäßigen Abständen (optional). Das Aktualiserungsintervall legen Sie bei der LDAP-Konfiguration in der iRMC S4-Web-Oberfläche fest (Seite in der Option *LDAP E-Mail Tabellen aktualisieren* (siehe Handbuch "iRMC S4 - integrated Remote Management Controller").

Globale E-Mail-Benachrichtigung auf dem Verzeichnisserver konfigurieren

Nachfolgend ist beschrieben, wie Sie die E-Mail-Benachrichtigung auf dem Verzeichnisserver konfigurieren.

Zusätzlich sind Einstellungen für den iRMC S4 erforderlich, die Sie an der iRMC S4-Web-Oberfläche konfigurieren (siehe Handbuch "iRMC S4 - integrated Remote Management Controller").

Gehen Sie wie folgt vor:

- Tragen Sie im Verzeichnisdienst die E-Mail-Adressen der Benutzer ein, an die E-Mails gesendet werden sollen.

  Das Verfahren zur Konfiguration der E-Mail Adresse unterscheidet sich je nach verwendetem Verzeichnisdienst (Active Directory, eDirectory und OpenLdap).

- Erstellen Sie eine Konfigurationsdatei, in der die Alert Roles definiert sind.

- Starten Sie den *SVS_LdapDeployer* mit dieser Konfigurationsdatei, um eine entsprechende LDAP v2-Struktur (*SVS*) auf dem Verzeichnisserver zu generieren (siehe Seite 243 und Seite 249).

8.2.8.2 Benachrichtigungsgruppen (Alert Roles) anzeigen

Nach der Generierung der LDAP v2-Struktur wird z.B. in Active Directory die neu angelegte OU *SVS* mit den Komponenten *Alert Roles* und *Alert Types* unter *Declarations* sowie mit der Komponente *Alert Roles* unter *DeptX* angezeigt (siehe Bild 82):

– Unter *Declarations* zeigt *Alert Roles* alle definierten Alert Roles an, *Alert Types* werden alle Benachrichtigungstypen angezeigt (1).

– Unter *DeptX* zeigt *Alert Roles* alle in der OU *DeptX* gültigen Alert Roles an (2).

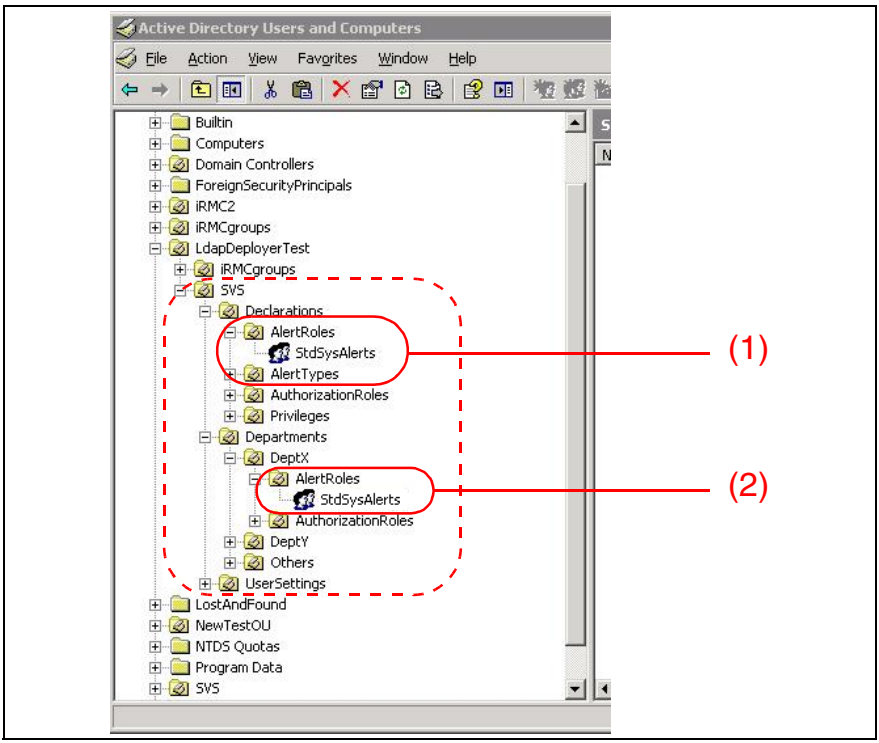


Bild 82: OU SVS mit Alert Roles

Damit an die Benutzer der einzelnen Benachrichtigungsgruppen E-Mails versendet werden, muss am iRMC S4 die zugehörige Abteilung (Department, in Bild 82: *DeptX*) konfiguriert sein (siehe Handbuch "iRMC S4 - integrated Remote Management Controller").

Wenn Sie im Strukturbaum von *Active Directory-Benutzer und -Computer* (siehe Bild 83) unter *SVS – Departments – DeptX – Alert Roles* eine Benachrichtigungsgruppe (Alert Role, z.B. *StdSysAlerts*) auswählen (1) und via Kontextmenü *Eigenschaften – Mitglieder* den *Eigenschaften*-Dialog für diese Benachrichtigungsgruppe öffnen, werden in der Registerkarte *Mitglieder* die Benutzer angezeigt (2), die der Benachrichtigungsgruppe (hier: *StdSysAlerts*) angehören.

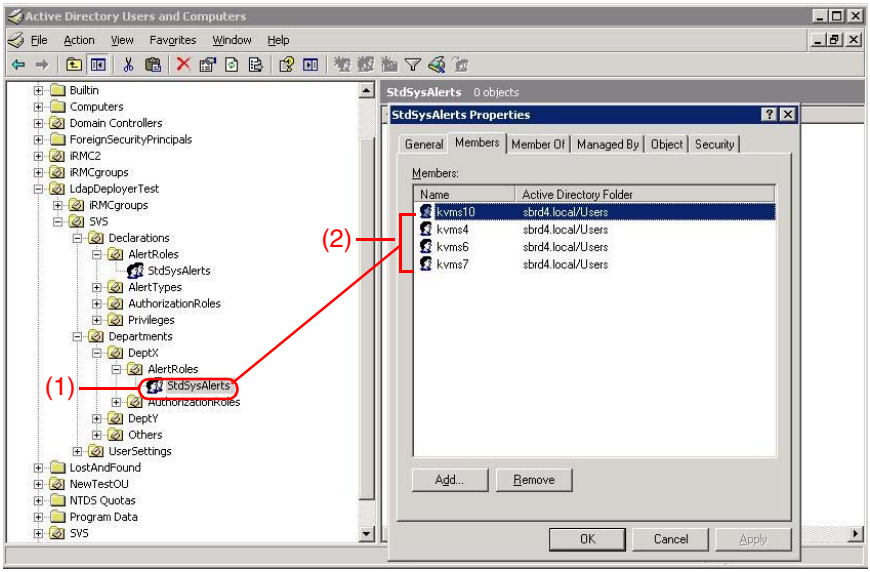


Bild 83: Benutzer mit der Alert Role „StdSysAlert“

8.2.8.3 iRMC S4-Benutzer einer Benachrichtigungsgruppe (Alert Role) zuordnen

Die Zuordnung von iRMC S4-Benutzern zu Benachrichtigungsgruppen (Alert Roles) können Sie wahlweise vornehmen

– ausgehend vom Benutzereintrag oder
– ausgehend vom Rolleneintrag.

In den einzelnen Verzeichnisdiensten (Microsoft Active Directory, Novell eDirectory und OpenLDAP) erfolgt die Zuordnung iRMC S4-Benutzern zu iRMC S4 Benachrichtigungsgruppen (Alert Roles) analog und mit denselben Tools wie bei der Zuordnung von iRMC S4-Benutzern zu iRMC S4-Berechtigungsgruppen (Authorization Roles).

In Active Directory z.B. treffen Sie die Zuordnung über die Schaltfläche *Add...* im *Eigenschaften*-Dialog des Snap-in *Active Directory Benutzer und -Computer* (siehe Bild 83 auf Seite 305).

8.2.9 SSL Copyright

Die iRMC S4-LDAP Integration verwendet die auf dem OpenSSL Project basierende SSL Implementation von Eric Young.

```
/* ====================================================================
 * Copyright (c) 1998-2002 The OpenSSL Project.  All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 *
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in
 *    the documentation and/or other materials provided with the
 *    distribution.
 *
 * 3. All advertising materials mentioning features or use of this
 *    software must display the following acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
 *
 * 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
 *    endorse or promote products derived from this software without
 *    prior written permission. For written permission, please contact
 *    openssl-core@openssl.org.
 *
 * 5. Products derived from this software may not be called "OpenSSL"
 *    nor may "OpenSSL" appear in their names without prior written
 *    permission of the OpenSSL Project.
 *
 * 6. Redistributions of any form whatsoever must retain the following
 *    acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
 *
 * THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
 * EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
 * PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
 * ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
 * SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
 * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
 * LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
 * STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
 * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
 * OF THE POSSIBILITY OF SUCH DAMAGE.
 * ====================================================================
 *
 * This product includes cryptographic software written by Eric Young
 * (eay@cryptsoft.com).  This product includes software written by Tim
 * Hudson (tjh@cryptsoft.com).
 *
 */
```

```
/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
 * All rights reserved.
 *
 * This package is an SSL implementation written
 * by Eric Young (eay@cryptsoft.com).
 * The implementation was written so as to conform with Netscapes SSL.
 *
 * This library is free for commercial and non-commercial use as long as
 * the following conditions are aheared to.  The following conditions
 * apply to all code found in this distribution, be it the RC4, RSA,
 * lhash, DES, etc., code; not just the SSL code.  The SSL documentation
 * included with this distribution is covered by the same copyright terms
 * except that the holder is Tim Hudson (tjh@cryptsoft.com).
 *
 * Copyright remains Eric Young's, and as such any Copyright notices in
 * the code are not to be removed.
 * If this package is used in a product, Eric Young should be given attribution
 * as the author of the parts of the library used.
 * This can be in the form of a textual message at program startup or
 * in documentation (online or textual) provided with the package.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the copyright
 *    notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in the
 *    documentation and/or other materials provided with the distribution.
 * 3. All advertising materials mentioning features or use of this software
 *    must display the following acknowledgement:
 *    "This product includes cryptographic software written by
 *     Eric Young (eay@cryptsoft.com)"
 *    The word 'cryptographic' can be left out if the rouines from the library
 *    being used are not cryptographic related :-).
 * 4. If you include any Windows specific code (or a derivative thereof) from
 *    the apps directory (application code) you must include an acknowledgement:
 *    "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
 *
 * THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
 * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
 * ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
 * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
 * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
 * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
 * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
 * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
 * SUCH DAMAGE.
 *
 * The licence and distribution terms for any publically available version or
 * derivative of this code cannot be changed.  i.e. this code cannot simply be
 * copied and put under another distribution licence
 * [including the GNU Public Licence.]
 */
```